CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

MARCH 2023

Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses

Steven Feldstein and Brian Kot

Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses

Steven Feldstein and Brian Kot

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary

The global spyware and digital forensics industry continues to grow despite public backlash following an array of surveillance scandals, many linked to NSO Group's Pegasus program. This paper explores the resilience of the commercial spyware market and offers ideas about how to limit the spread of invasive cyber surveillance tools. It highlights several factors driving the industry, including elevated demand for intrusion technology from government clients and private customers, as well as inconsistent political will from democratic governments to crack down on these technologies.

Key Insights

- Between 2011 and 2023, at least seventy-four governments contracted with commercial firms to obtain spyware or digital forensics technology, according to data collected by Carnegie's global inventory of commercial spyware and digital forensics (*https://data.mendeley.com/datasets/csvhpkt8tm/10)*.

- Autocratic regimes are much likelier to purchase commercial spyware or digital forensics than democracies: forty-four regimes classified as closed autocracies or electoral autocracies procured targeted surveillance technologies between 2011 and 2023, contrasted with thirty electoral democracies or liberal democracies.

- Israel is the leading exporter of spyware and digital forensics tools documented in the global inventory: fifty-six out of seventy-four governments have procured commercial spyware and digital forensics technologies from firms that are either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru.

- In addition to top-level commercial spyware vendors like NSO Group and Cytrox, there is a burgeoning secondary tier of suppliers composed of boutique spyware firms, hacker-by-night operations, exploit brokers, and similar groups. As large commercial firms face greater scrutiny from democratic governments about their practices, there is a corresponding increase in open-source and commercially available malware. These trends have made it less costly for governments and private actors to mount attacks and allow them to hide in the "noise" of open-source codes and gain plausible deniability.

- Ongoing high demand for intrusion technology contributes to the resilience of the commercial spyware and digital forensics market. Even if one supplier is sanctioned, there is sufficient financial motivation for other suppliers to fill in the gap. Our data set shows that governments have transitioned from procuring spyware from older suppliers, like FinFisher and Hacking Team, to contracting with alternatives, such as NSO Group, Cytrox, and Candiru.

- Democratic governments have been inconsistent in tackling the human rights abuses enabled by spyware. In the European Union (EU), cybersecurity companies exploit regulatory fragmentation to establish offices in member states where implementation of export controls is known to be weak. For example, NSO Group established subsidiaries in Bulgaria and Cyprus to facilitate selling its products. Intellexa, which owns a number of surveillance firms, including Cytrox and Circles, established footholds in Cyprus, Greece, and Malta. The EU should push for more consistency and minimum standards of enforcement when it comes to governing the licensing and export of intrusive technology.

- Spyware companies routinely cover their tracks by creating complex corporate structures to obfuscate their legal registration, what laws they are bound by, and who their clients are. Governments in Europe, Israel, the United States, and other relevant jurisdictions should enhance their policy and regulatory cooperation on spyware. They should improve their information-sharing and create unified registries of cyber surveillance firms.

- Recent developments—such as the U.S. blacklisting of NSO Group in 2021, which has driven the firm to the verge of bankruptcy—illustrate how economic leverage can force the industry to reckon with the consequences of human rights violations. The United States should seek to multilateralize the Entity List with regard to spyware companies. A good starting point would be to pressure European countries to set up a parallel entity list and to similarly sanction NSO Group, Candiru, and related firms.

- The United States should reconsider its current permissive approach toward digital forensics and data extraction technologies. Researchers have documented over two thousand U.S. law enforcement agencies that have procured digital forensics technology to investigate criminal cases. While these tools require physically confiscating a target's device, the level of intrusiveness is comparable to if not greater than that of remote spyware technology. Like spyware, phone extraction enables full, retroactive access to files and messages, as well as metadata about past communications.

- As a leading exporter of spyware, Israel has not sufficiently prioritized human rights considerations in its export licensing regime. The United States and other democracies should continue to use economic and diplomatic leverage to pressure Israel to restrict commercial spyware transactions to human rights–abusing countries.

Introduction

In 2021, sixteen media outlets formed a consortium known as the Pegasus Project to investigate military-grade spyware licensed by the Israeli firm NSO Group. Two of the consortium partners, Forbidden Stories and Amnesty International, had gained access to a list of fifty thousand phone numbers that were "selected for targeting" by NSO clients. The group analyzed the numbers and matched them to specific individuals and hacks. The findings were damning. From the original list, analysts identified over one thousand targeted individuals spread across over fifty countries. Victims included "several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials — including cabinet ministers, diplomats, and military and security officers."[1] At least ten prime ministers, three presidents, and one king were also found on Pegasus target lists. The investigation sent shockwaves around the world. It fueled public outrage and compelled the United States to blacklist NSO Group—driving the firm to the brink of bankruptcy.[2]

While NSO Group's future is in doubt, the spyware industry as a whole remains relatively unscathed. Governments have turned to other commercial firms to accomplish their surveillance objectives. Cytrox's Predator spyware, for example, has become a favored option for many governments and was recently the subject of investigations in Greece, following disclosures that government operators used Predator malware to hack the phones of journalist Thanasis Koukakis and opposition leader and member of the European Parliament (MEP) Nikos Androulakis.[3] In addition to Greece, researchers have found that state-backed operators in Armenia, Côte d'Ivoire, Egypt, Indonesia, Madagascar, Serbia, and Spain are likely also using Predator.[4] In a striking example, researchers from the Citizen Lab discovered that Egyptian operators were "simultaneously" using Pegasus and Predator spyware to hack the phone of opposition politician Ayman Nour.[5]

These incidences reinforce two core facts: that the spyware industry is bigger than any single company, and that governments are highly motivated to acquire these tools, even at the risk of public backlash.

The Pegasus Project investigation isn't the first time that mercenary spyware firms have faced setbacks. Years before the Pegasus scandal, Germany's FinFisher and Italy's Hacking Team were dominant players in the market. Products from both companies were linked to surveillance abuses in a range of countries. At its height in 2015, Hacking Team's products were in use in forty-one countries.[6] Yet by March 2022, FinFisher had shut down its operations because of financial insolvency, following raids by German authorities and an accompanying investigation into the company.[7] As for Hacking Team, the firm suffered a massive 400-gigabyte data breach in 2015 that revealed "executive emails, customer invoices and even source code."[8] The firm has struggled to recover from that episode. It has changed ownership and rebranded itself as Memento Labs but has acquired few new clients.[9] While the demise of FinFisher and Hacking Team (and potentially NSO Group) shows that public investigations and advocacy campaigns can be effective, the industry's resilience extends beyond individual firms. The collapse of these companies has done little to curtail global sales—estimated to be worth over $12 billion—and other spyware vendors continue to vie for government contracts and private customers.[10]

The paper begins by reviewing the international legal and policy standards governing the use of spyware surveillance. It then describes overall trends in the commercial spyware and digital forensics market and presents a global inventory of these tools.[11] The inventory evaluates which governments have acquired commercial spyware and digital forensics technologies, how states are using these tools, which companies are selling spyware and digital forensics, and where these firms are headquartered. Next, the paper examines the continued resilience of the global spyware industry and discusses which factors have allowed the market to persist and thrive in such places as the EU and Israel. Lastly, the paper discusses policy responses and steps democracies can take to impose limits on the spyware industry.

When Is It Permissible for Governments to Use Spyware?

Spyware capabilities are immensely invasive. The software allows operators to gain remote access to devices so they can target individuals from almost any part of the world. Once an operator infects a device, that agent gains "complete and unrestricted access to all sensors and information on infected devices, effectively turning most smartphones into 24-hour surveillance devices."[12] Hacking represents a serious violation of the right to privacy and can

be a deeply distressing experience for victims. Spyware is also a tool of intimidation for journalists, activists, and opposition politicians, serving to suppress media reporting, intimidate critics, or dissuade regime challengers from running in an election. Spyware allows agents to "get inside a political exile's entire network without setting foot inside the target's adopted country" while avoiding the attendant risks associated with traditional espionage.[13] For this reason, the use of spyware features heavily in transnational repression. One of the most notorious cases was the assassination of exiled Saudi journalist Jamal Khashoggi in the Saudi consulate in Türkiye. After the killing, investigators examined the phones of close associates of Khashoggi's and discovered that the devices were infected with Pegasus. Saudi security operatives likely used this information to help plan and execute Khashoggi's murder.[14]

Limited circumstances can justify the use of intrusive surveillance techniques—such as preventing or investigating a specific serious crime or an act constituting a grave threat to national security. International law holds that targeted surveillance measures should be narrowly tailored to investigate specific individuals suspected of committing serious crimes or acts threatening national security. Spyware should be deployed as a last resort, after "all less intrusive measures should have been exhausted or have been shown to be futile."[15] And the duration and scope of spyware use should be strictly limited only to relevant data. In short, governments should comply with principles of "legality, necessity, and proportionality" when using cyber surveillance technologies.[16] But governments rarely adhere to these standards. States exploit national security or public order rationales to give their law enforcement agencies a wide berth to deploy intrusive software against an array of targets, with little regard to the principles of necessity and proportionality. Once those agencies obtain spyware, there are few guardrails governing its use. As David Kaye, the former United Nations (UN) special rapporteur for freedom of opinion and expression wrote:

> It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not.[17]

Empirically, both authoritarian states and democracies routinely conduct unlawful surveillance against a host of illegitimate targets—political rivals, meddlesome journalists, or government critics. Zero-click software like Pegasus, which does not even require a victim to click on a compromised link or install a corrupted file, offers powerful temptations for political leaders to expand the net of surveillance. While there is growing public pressure among a small group of liberal democracies, such as Greece and Spain, to end their abuses, this is the exception. For the bulk of governments that deploy spyware, there is little likelihood that they will change their behavior. This has led prominent jurists, such as Dunja Mijatović, commissioner for human rights of the Council of Europe, to question whether there are any circumstances that should permit the use of spyware. She observes that tools like Pegasus are

a "game-changer in digital surveillance" and that it is "virtually unimaginable that the use of Pegasus or equivalent spyware could ever be considered in accordance with the law and the necessary safeguards as outlined by the [European Court of Human Rights]."[18]

Spyware operations can be broken down into a couple of categories: 1) national in-house operations and advanced persistent threat (APT) groups—high-capacity actors who carry out sustained intrusion attacks over a prolonged period of time—and 2) commercial spyware vendors.[19] Operations in the first category are often carried out by highly capable states, such as the National Security Agency's "tailored access operations" group, Israel's Unit 8200, and equivalent Chinese or Russian actors that receive direct or tacit government support. These activities are conducted in a clandestine manner and are challenging to scrutinize. They are not the focus of this paper.

Instead, this paper scrutinizes activities occurring in the second category: commercial spyware sold for profit to government and private clients. These products do not require actors to possess in-house capacity to develop or carry out cyber surveillance attacks. Instead, governments purchase these capabilities directly from companies, which provide after-sales support, such as technical upgrades, product updates, trainings, and related customer services.[20] The emergence of the commercial spyware sector has given a wide range of countries the means to acquire advanced surveillance tools they would otherwise struggle to obtain.

Global Context of Commercial Spyware and Digital Forensics

The global spyware and digital forensics industry is booming, bringing record profits in the billions of dollars. In December 2020, Steven Feldstein released a global inventory of commercial spyware that was subsequently included in the book *The Rise of Digital Repression*.[21] The inventory revealed that at least sixty-five governments, both authoritarian and democratic, had contracted with commercial spyware vendors. While not all uses led to abuses, many incidences were linked to major human rights violations. Two years later, we have revised the global inventory and released a new version. The current data set, presented in Appendix 1, which incorporates incidents from 2011 to 2023, includes several important changes:[22]

- Incorporates two categories of targeted surveillance technologies: spyware and digital forensics (physical tools used to breach digital devices in order to extract and analyze stored data). It does not include other types of targeted surveillance, such as network monitoring or lawful interception technologies.

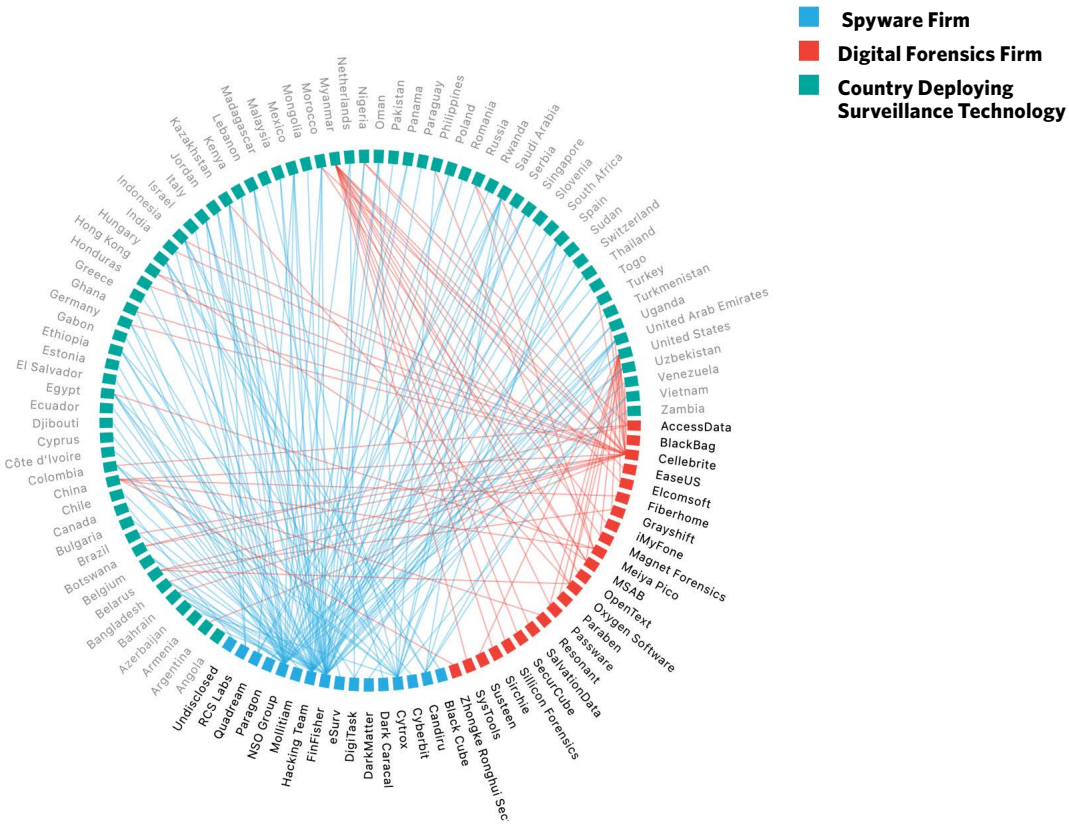
- Organizes the data set by event type in separate entries rather than aggregating commercial spyware firms by country.

- Takes advantage of the wider scrutiny of the spyware industry in the past two years, which has generated more details and sourcing about new vendors and operations.[23]

The results of the latest data set show that at least seventy-four governments have contracted with commercial firms to obtain spyware or digital forensics technology.

Three companies—NSO Group, FinFisher, and Hacking Team—appear most frequently in the updated data set. This is likely due to two factors: 1) all three companies have registered significant sales and transactions and have been market leaders at various times and 2) as a result, journalists have focused intensively on transactions linked to those companies, possibly overlooking other vendors (in the case of Hacking Team, its 2015 data breach gave journalists far more information to work with than they had for competing firms). In terms of government clients, the data shows that autocratic regimes are far likelier to purchase commercial spyware or digital forensics than democracies: forty-four regimes classified

Figure 1. Key Relationships Between Governments and Intrusion Technology Firms



Note: To view the interactive graphic, please visit https://carnegieendowment.org/programs/democracy/commercialspyware.

as closed autocracies or electoral autocracies procured targeted surveillance technologies between 2011 and 2023, contrasted with thirty electoral democracies or liberal democracies. Finally, when it comes to countries of origination, Israel is the leading exporter of spyware and digital forensics tools, with Italy and Germany a distant second and third (the latter two countries' ranks are mostly due to the past presence of FinFisher and Hacking Team). Figure 1 visually depicts the global distribution of spyware and digital forensics surveillance vendors, exporting countries, and procuring governments.

Public scrutiny has tended to focus on top-level commercial vendors—entities like NSO Group, which are capitalized by international private equity firms. These companies offer the most sophisticated products, particularly zero-click infections, which are expensive to obtain and difficult to detect. Zero-click infections allow operators to install malware on a device without the victim having to click on a compromised link or install a corrupted file. These infections exploit security flaws in operating systems such as Apple's iOS or Google's Android. By simply sending a message via communications apps like Signal, iMessage, or WhatsApp, operators can remotely execute malicious codes and take control of a victim's entire device.[24] In addition to providing state-of-the-art exploits—pieces of software or code designed to take advantage of cybersecurity flaws—for customers to use against devices, firms like NSO Group offer a full package of support for clients, ranging from monitoring targets and exploitation services to ongoing servicing.

Not many companies can match the capabilities of NSO Group or Cytrox, but that may not matter. Beneath the top tier of companies lies a burgeoning secondary tier of suppliers composed of boutique spyware firms, hacker-by-night operations, exploit brokers, and similar groups. As commercial firms face greater scrutiny from democratic governments about their practices, there has been a corresponding increase in open-source and commercially available malware, which has made it easier for groups to mount attacks.[25] Many of these firms are based in countries like India, the Philippines, and Cyprus. And while these tools have been described as the surveillance equivalent of "strip-mall phone repair shops,"[26] Meta's threat intelligence team observes that a "growing number" of APT groups are choosing to rely on openly available spyware tools, including open-source malware from sources such as GitHub, rather than procure more sophisticated offensive capabilities.[27]

There are a couple of reasons behind this shift. For one, these tools cost far less than customized exploits for sale by large commercial firms. Even if they fail to accomplish an organization's objectives, obtaining new options takes minimal resources and energy. For example, Meta's threat team documents a hacker organization based in Pakistan, known as APT36, that directed attacks against government, military officials, and activists. Their goal was to trick targets into installing malware to compromise their devices. To obtain the malware, APT36 simply downloaded a free tool from GitHub called XploitSPY, which they lightly modified.[28] Some European companies also rely on open-source codes to craft intrusive software. GR Sistemi, an Italian surveillance tech company, created its Dark Eagle spyware

by repackaging an open-source remote access trojan called AndroRAT.[29] A Germany-based intelligence company called Wolf Intelligence built its WolfRAT malware using "copy + pasted open source resources."[30] In addition to repurposing openly available sources, it is not uncommon for surveillance firms to copy and recycle their counterparts' codes. FinFisher has been accused of plagiarizing FlexiSpy, a cheap malware created by a Thai firm to help customers monitor their spouses; Hacking Team allegedly subscribed to multiple consumer malware services "to learn about new intrusion techniques."[31]

Groups that rely on low-cost, open-source tools are able to hide in the "noise" and maintain plausible deniability about which organization was culpable for launching the attack. Casey Newton writes, "malware created by state actors often carries telltale signs of who developed it in its code; when everyone is using the same code, though, platforms lose an important signal. . . . If a bunch of different threat actors are throwing the same malware all over the internet, it makes it harder for analysts to pull together exactly who is behind it."[32] This helps explain why in certain situations, actors may actually prefer to use commonly sourced code for malware intrusion attacks, rather than to deploy commercial spyware alternatives. The arrival of OpenAI's ChatGPT tool could open the door to further malfeasance: cybersecurity researchers have been able to get the text generation tool to write phishing emails and malicious code.[33]

Digital Forensics: Different Tools, Similar Outcomes

The global inventory also documents government use of phone extraction or digital forensics technologies. Unlike traditional spyware, phone extraction requires physically confiscating a target's device, making this technique less suited for transnational repression. Nonetheless, the level of intrusiveness is comparable to if not greater than that of remote surveillance technology.[34] Like spyware, phone extraction enables full, retroactive access to files and messages, as well as metadata about past communications. By establishing a physical connection with the targeted mobile device, forensic hardware (such as Cellebrite's Universal Forensic Extraction Device, or UFED) is capable of penetrating most security features in order to extract a full copy of data from a cell phone, even when the phone is locked.

A technique called physical extraction can be particularly invasive. By analyzing bit-by-bit a device's full physical storage, physical extraction techniques can retrieve even "deleted" data from phones (deleted information often leaves behind a footprint in free storage space).[35]

Other products, like Grayshift's GrayKey, utilize an exploit to bypass password-guessing limits, allowing law enforcement agencies to apply brute force to penetrate password controls and gain access to a particular device.[36] The booming use of cloud storage heightens the risk that intruders can access troves of personal data even if only one device is compromised. Depending on various factors (such as the type of device, security setting, cloud account setting, and operational security), a user of these methods may obtain partial or complete access to extensive categories of data stored on the device, including contacts, call metadata, SMS messages, stored files, app data, location data, Wi-Fi networks, and keychain data.[37] Unsurprisingly, these tools have become indispensable to law enforcement. In the United States alone, researchers have documented more than two thousand law enforcement agencies across local, state, and federal levels that have procured phone extraction technology to investigate cases of not just violent crimes but also minor offenses like shoplifting and graffiti.[38] They include municipal police departments, local sheriffs' departments, state departments of public safety, and local and federal district attorneys. Such widespread use is problematic because there are few guidelines to clarify when deploying these tools represents an unlawful overreach of civil liberties. In the absence of regulation, it is left to individual officers or agencies to determine appropriate use—a situation that lends itself to abuse.

The similarity between digital forensics tools and remote-control spyware becomes apparent when considering use cases. While phone-cracking and spyware companies assert that they exclusively sell their products to law enforcement agencies tackling crime and terrorism, in practice, they sell their products indiscriminately, failing to adhere to minimal standards of human rights due diligence. For example, despite Cellebrite's claim to "prioritize a human rights-based approach," the company's clients include some of the most repressive regimes in the world.[39] Sources indicate that Cellebrite has sold its data extraction technologies to at least twenty-three governments, including such egregious human rights abusers as the governments of Bahrain, China, Myanmar, Saudi Arabia, and the United Arab Emirates (UAE).[40]

Explaining the Resilience of the Global Spyware and Digital Forensics Industry

Despite growing public criticism of intrusion software, the sector as a whole continues to flourish. There is some debate about how to handle the industry—many advocates and institutions, including the UN human rights agency, have called for a moratorium on the sale or use of spyware tools "until a human rights-based safeguards regime is in place."[41]

As it stands, the intrusion surveillance market is largely unregulated. It is rife with abuse, allowing governments and private actors to deploy surveillance tools with impunity against human rights defenders, journalists, and opposition politicians. There is a strong consensus that the intrusion technology market requires greater accountability and much more oversight. Yet, despite growing public criticism, it continues to operate in an unchecked manner. Public campaigns, surveillance scandals, and policy directives have manifestly failed to constrain the market. What explains this lack of success?

Part of the problem is rooted in the political economy of the spyware market. Simply put, demand for spyware technology remains extraordinarily high—whether from government clients or private companies. Even if one supplier is sanctioned, there is sufficient financial motivation for other suppliers to fill in the gap. The data appears to bear this out. Looking at the different firms that have risen and fallen over the last eleven years, the global inventory shows a clear transition from older suppliers, like FinFisher and Hacking Team, to newer entrants—NSO Group, Cytrox, Candiru, and so forth. While efforts to rein in specific companies have achieved some success, it is unclear whether these actions have dampened overall market demand for spyware. It is possible that recent scrutiny of NSO Group (as well as Cytrox) may reduce the reach of the largest commercial vendors. But as discussed, even if most top-tier firms were put out of business (an unlikely outcome), this would still not shut down the market. Rather, it would hasten decentralization and increase opportunities for boutique firms and informal hacker-for-hire operations to fill in the gap. The fact remains, as long as repressive leaders, unscrupulous law enforcement agencies, and disreputable private companies seek to acquire these tools, the market will respond accordingly. That being said, there is a significant difference in capability between second-tier hacking-for-hire tools and top-of-the-line software from entities like NSO Group. If the result of greater market regulation is to force countries like Egypt or the UAE to procure more rudimentary spyware from boutique operators, this would be a beneficial outcome.

A second problem is that democratic governments have sent mixed messages about whether they are genuinely interested in cracking down on intrusion technology. The European Union is a good example. Despite its relatively stringent rules regulating spyware exports and sales, Europe is a nexus of these technologies. An abundance of domestic commercial spyware companies are based in European countries; these firms develop and sell advanced intrusive technology in their home markets and overseas. An Italian firm, Tykelab/RCS Lab, for instance, has helped clients surveil phone networks in countries such as Costa Rica, Greece, Iraq, Kazakhstan, Libya, Malaysia, Mali, Nicaragua, and Portugal (as well as within Italy itself).[42] Sweden's MSAB, a digital forensics firm and a rival to Cellebrite, has sold its phone-cracking technology to governments in Hong Kong, Morocco, Myanmar, and the United States. Meanwhile, the Austria-based company DSIRF has developed a zero-day malware used to surveil individuals in Austria, Panama, and the United Kingdom.[43]

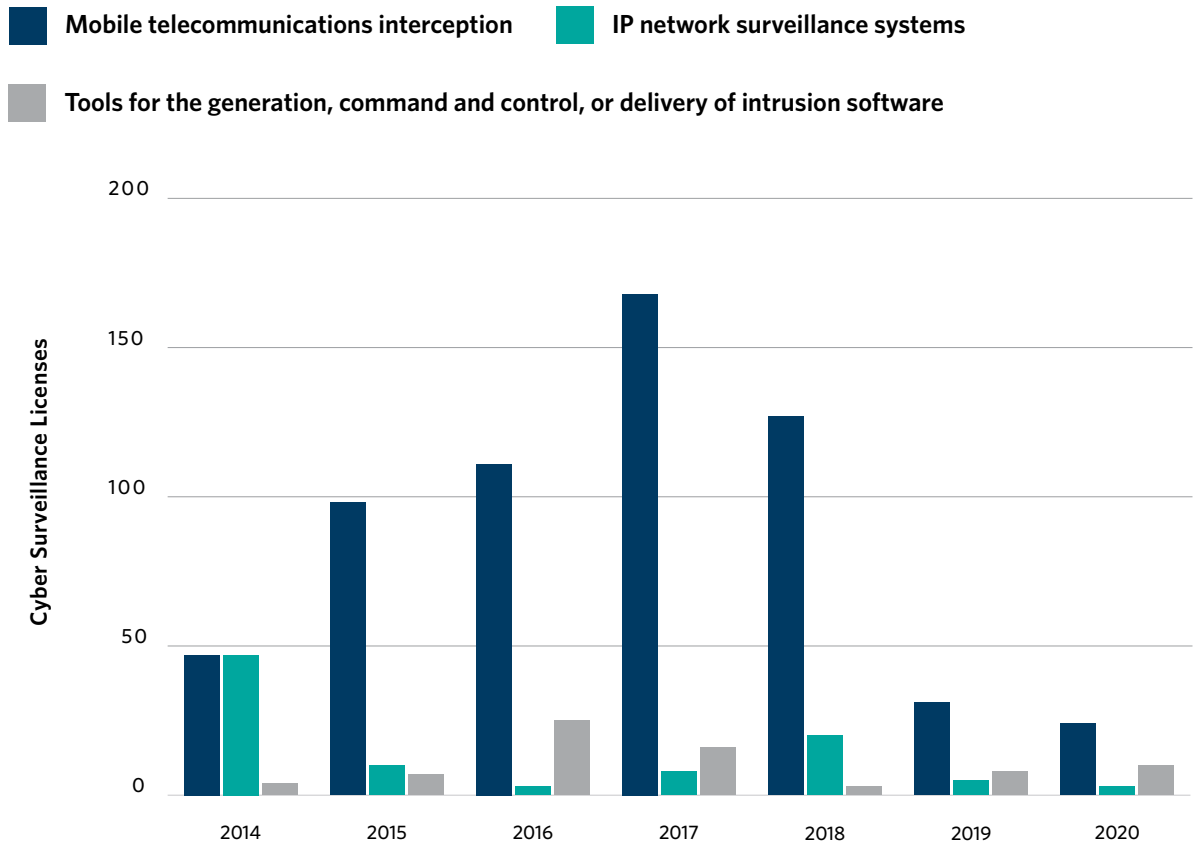
In theory, the EU has strict rules of export, but member states can easily get around them due to what Sophie in 't Veld, the rapporteur for the European Parliament's PEGA Committee (which investigates the use of Pegasus and equivalent spyware), characterizes as "deliberate lax national implementation."[44] Companies commonly establish subsidiaries in member states that are willing to overlook spyware operations to evade EU controls. Council Regulation (EC) No. 428/2009 is supposed to ensure consistency across EU member states when it comes to controlling dual-use items, including intrusion software, but in practice, cybersecurity companies take advantage of regulatory fragmentation to establish offices in member states where implementation of export controls is known to be weak.[45] For example, NSO Group established subsidiaries in Bulgaria and Cyprus to facilitate selling its products.[46] Intellexa, which owns a number of surveillance firms, including Cytrox and Circles, established footholds in Cyprus and Greece.[47] Authorities in both countries have refused to disclose Intellexa's legal filings for non-EU sales. In 't Veld notes that "each time the regime for export licenses was tightened in Israel, several companies moved their export departments to Europe, in particular Cyprus."[48]

For instance, in January 2023, *Haaretz* reported that the firm Passitora, controlled by Israeli businessman Tal Dilian and part of the Intellexa alliance, sold mobile intercept surveillance equipment to Bangladesh's National Telecommunication Monitoring Center (NTMC). The agency monitors internet and social media use, allegedly "eavesdropping on opposition officials, protestors and ordinary citizens." Bangladesh is not on Israel's approved licensing list of countries for the export of sensitive technology. To get around this hurdle, Dilian incorporated a subsidiary in Cyprus (which he later relocated to Greece after he got into hot water with the Cypriot government) and exploited loose export regulations to send the equipment to Bangladesh and to later host surveillance trainings for NTMC officials in Greece.[49]

As it stands, EU legislation does not require member states to assess the adequacy of their legal frameworks when it comes to exporting spyware to countries of destination: "Indeed, there is no need to even consider if the end-use of the technology by the end-user is lawful in the importing jurisdiction."[50] The results are stark; member states have historically approved the "vast majority" of export licenses for cyber surveillance items.[51] Research by Security for Sale shows that member states permitted surveillance technology exports at least 317 times between 2015 and 2017, while rejecting only fourteen applications.[52] Notably, EU member states appear to be tightening their licensing procedures; in 2019, member states granted forty-four licenses for listed cyber surveillance items, while issuing eighty-one denials.[53] Figure 2 shows licensing approvals granted by the EU for cyber surveillance items between 2014 and 2020.

EU agencies, institutions, and member states also circumvent the bloc's own rules when it comes to exporting and transferring intrusive technologies. In a December 2022 hearing organized by the European Parliament, Ilia Siatitsa from Privacy International explained how EU institutions have facilitated the "direct transfer of surveillance equipment to third countries," as well as financing and training security services in the use of these tools.[54] Siatitsa noted that EU bodies have even promoted legislation in third countries to enable

Figure 2. Cyber Surveillance Licenses Granted by the EU, 2014–2020



Source: *Report from the Commission to the European Parliament and the Council on the Implementation of Regulation (EU) 2021/821 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer Of Dual-use Items* (Brussels: European Commission, November 2021), 6, https://trade.ec.europa.eu/doclib/docs/2021/november/tradoc_159936.pdf.

surveillance.[55] In one example, Privacy International discovered that in a training session supported by the EU, the national police force of Spain promoted the use of malware or computer trojans to law enforcement authorities in Bosnia and Herzegovina. In another instance, EU allocations from the Emergency Trust Fund for Africa allowed Niger's government to acquire mobile interception technology, despite the government's record of human rights violations. This transaction occurred due to the European Commission's failure to carry out a risk assessment prior to agreeing to support projects with surveillance implications.[56]

On the demand side, European democracies have procured commercial spyware for many years. In 't Veld writes, for example, that twenty-two end users in at least fourteen EU member states have acquired Pegasus. Export regulators often consider EU membership to be a sufficient guarantee for compliance with the highest standards of human rights and

exempt EU countries from further human rights due diligence. Israel's export authority, for instance, does not require EU member states to submit individual human rights assessments, which are normally required, when they apply for export licenses.[57] But this presumption of compliance is clearly insufficient, considering the pattern of abuses occurring in countries like Greece, Hungary, and Spain.[58] In fact, Spanish authorities have been embroiled in a sprawling spyware scandal, with more than sixty-five individuals targeted or infected by Pegasus or Candiru malware between 2017 and 2020.[59] The victims—representing large swaths of Catalonia's civil society, government, and elected officials—were likely targeted by Spain's national government for their support for Catalan independence. Part of spyware's appeal, including for European law enforcement, is that it allows operators to circumvent end-to-end encryption, which Ronald Deibert notes has become a "growing barrier to government mass surveillance programs that depend on the collection of telecommunications and Internet data."[60] Spyware offers a workaround, permitting agents to get inside a user's device in order to read communications, access confidential documents, or listen in on calls before encryption or after decryption.[61] Spyware's prevalence in Europe, both as a tool of export and as an instrument of domestic surveillance, is a powerful reminder that surveillance abuses are not unique to authoritarian regimes. All countries, regardless of regime type, are susceptible to misusing spyware when safeguards and oversight are absent or inadequate.

Israel is another major exporter of commercial intrusive technologies. Our inventory shows that fifty-six out of seventy-four governments have procured spyware and digital forensics technologies from firms that are either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru.

Israel's prominence in the intrusion technology market is not surprising. The country's spyware industry has benefited from the diffusion of technical know-how from its defense establishment. A study cited by *Haaretz* claims that 80 percent of the 2,300 people who founded Israel's seven hundred cyber companies had served in Israel Defense Forces (IDF) intelligence units, notably Unit 8200.[62] As reported by the *New York Times*, nearly every member of NSO Group's research team has worked at some level of the Israeli Military Intelligence Directorate.[63] Similarly, the founders of spyware firm Candiru—Eran Shorer and Yaakov Weizman—reportedly served in Unit 8200 and worked at NSO Group before establishing a rival business.[64] Tal Dilian, the founder of Intellexa, an alliance of cyber surveillance companies which includes Cytrox, served as a commander for the IDF's Unit 81, an entity responsible for developing intelligence tools for the IDF's special operations units and for other defense agencies.[65]

Israel's government maintains significant leverage over private cybersecurity firms through export control regulations. Under the 2007 Defense Export Controls Law, manufacturers of cyber weapons are required to obtain export licenses from the Ministry of Defense to sell their products abroad. Geopolitical interests play a role in determining whether licenses

will be granted.[66] For example, in March 2022, Israel's Defense Exports Controls Agency blocked Ukraine from purchasing Pegasus and restricted Estonia from using Pegasus against Russian targets.[67] Reportedly, Israeli officials were concerned that these sales could "provoke a confrontation" with Russia, whose military has been supporting the Syrian government's campaign to extinguish the remnants of the 2011 rebellion against President Bashar al-Assad—operations which are occurring near Israel's northeastern border.[68] Russia has also allowed Israel to confront Iran and Hezbollah in Syria, an arrangement that could be jeopardized if Israel were to assist Ukraine against Russian forces.[69] And when the United States blacklisted NSO Group and Candiru in 2021, Israeli officials lobbied Washington to take the companies off the blacklist. They maintained that the companies' activities were "of great importance to the national security of both countries" (Israeli officials were reportedly willing to commit to "much tighter supervision on licensing the software" if the United States lifted the ban).[70]

Setting Limits

The proliferation of commercial intrusion technology remains a pressing problem worldwide. As our global inventory shows, more countries than ever are deploying targeted surveillance tools for a variety of objectives—many of which directly reinforce repressive political ends. Democracies are some of the worst offenders, particularly when it comes to allowing dubious companies to set up shop, exploit regulatory loopholes, ship products to bad actors, and summarily rake in profits. While high demand for spyware will likely keep the industry afloat in the near term, that does not mean policymakers' hands are completely tied. The most realistic scenario to curb government abuse of spyware is to focus on supply-side strategies to limit states' abilities to acquire intrusion software. This means requiring spyware and digital forensics companies to stop selling their tools to the most egregious human rights offenders, or to force vendors to implement mandatory human rights due diligence requirements. Recent developments, such as the U.S. blacklisting of NSO Group in 2021—which has driven the firm to the verge of bankruptcy—illustrate how economic leverage can force the industry to reckon with the consequences of human rights violations.[71] These actions offer hope that political will is starting to build. But meaningful change will not occur without a genuine recognition from democratic policymakers that the harms from spyware outweigh its political, financial, or geopolitical benefits.

It is worth noting that while authoritarian regimes make up the majority of government spyware clients, most commercial spyware and digital forensics technology stems from Western companies based in liberal democracies. Israel, Europe, and the United States are

home to numerous firms that have relentlessly exploited legal loopholes and used complex and opaque corporate structures to evade accountability. The maneuverings undertaken by Dilian illustrate just how far certain individuals will go to find friendly jurisdictions that will turn a blind eye to their activities.

Thus, a useful starting point to hold the industry accountable is for governments in Europe, Israel, and the United States to enhance their policy and regulatory cooperation on intrusion software. Mandating that companies exhibit more transparency about their ownership structure and where they are headquartered would bring considerable benefits. Spyware companies routinely cover their tracks by creating complex corporate structures to obfuscate their legal registration, what laws they are bound by, and who their clients are. After a scandal comes to light, firms will rebrand or rename themselves to create distance from the allegations. An investigative analysis from Lighthouse Reports sheds light on Dilian's web of companies:

> Three companies called Intellexa were registered, in Greece, Ireland and the British Virgin Islands. All three were owned by an Irish holding company, Thalestris. As Inside Story dug into company registers in Greece and Cyprus they found that Thalestris also controlled companies named Apollo, Hermes, Mistrona, Dernova, Lorenco and Feroveno — some of which were seemingly registered to a rubble-strewn vacant lot in downtown Limassol. Thalestris, in turn, was partly dependent on money from another Virgin Islands entity, Chadera Enterprises, which — behind a veil of anonymity — was ultimately controlled by Dilian and two of his associates, leaked documents reveal.[72]

Individuals like Dilian are adept at hopscotching between jurisdictions to evade accountability. An important means to counter this strategy of "deliberate corporate obfuscation" is for Europe, Israel, the United States, and other relevant jurisdictions to improve their information-sharing and create unified registries of cyber surveillance firms.[73]

When it comes to the EU, the bloc suffers from fragmentation. Certain member states are reluctant to enforce basic regulations governing the licensing and export of spyware. Countries like Bulgaria, Cyprus, Greece, Hungary, Italy, and Malta are havens for spyware companies—which operate with minimal oversight. The problem has become so acute that it is common practice for firms to relocate from other jurisdictions, whether from adjoining EU member states or externally, to take advantage of loose export laws. This is a clear vulnerability; it behooves the European Council to push for more consistency and minimum standards of enforcement. But the problem is more than just fragmentation; European policymakers are disinterested in acting. In 't Veld writes: "The European Council and the national governments are practicing omertà. There has not been any official response to the scandal by the European Council. Member State governments have largely declined the invitation to cooperate with the PEGA committee. Some governments downright refused to cooperate."[74] In Greece, following a four-day visit by the PEGA Committee to investigate

evidence of broken laws related to the country's Pegasus scandal, a senior official contemptuously uttered: "We piss on PEGA."[75] It is difficult to envision meaningful change taking root until this policy calculus shifts.

The situation in the United States is more promising. The blacklisting of NSO Group and Candiru not only hamstrung two major spyware players, but also served as a warning shot to other companies in the industry. A forthcoming executive order prohibiting U.S. government use of commercial spyware "that poses counterintelligence or security risks to the United States or risks of being used improperly" is another auspicious development.[76] President Joe Biden's administration can take further steps to build on this progress.

First, Washington should seek to multilateralize the Entity List with regard to spyware companies. A good starting point would be to pressure European countries to set up a parallel entity list and to similarly sanction NSO Group, Candiru, and other firms.

Second, the United States should reconsider its current permissive approach toward digital forensics technologies. While there is a growing norm against law enforcement agencies using spyware, the same cannot be said for data extraction techniques. Over two thousand U.S. law enforcement agencies have procured digital forensics technology to investigate criminal cases.[77] The privacy consequences and potential harms from these tools are significant. These technologies allow agents to access extensive categories of data stored on devices, including contacts, call metadata, SMS messages, photos, stored files, app data, location data, Wi-Fi networks, and keychain data. At a minimum, the Biden administration should mandate a comprehensive privacy review of these technologies, evaluating the potential for overreach and abuse. Further, given the large number of U.S. companies exporting digital forensics products overseas—including to authoritarian regimes—enacting a temporary export ban (until the administration has implemented stricter licensing requirements) would be reasonable.

Third, and more difficult, the United States should take a harder stance when it comes to establishing intelligence and cybersecurity partnerships with governments that are known abusers of spyware technology. The recent agreement spearheaded by the United States to expand cybersecurity cooperation under the Abraham Accords is a good case in point. In January 2023, the United States announced it was broadening its collaboration on "cyberdefense" to include Bahrain and Morocco to the existing partnership between the United States, Israel, and UAE.[78] Bahrain, Morocco, and the UAE have faced extensive criticism for deploying spyware against government critics and journalists. As Deibert notes, "All of them have a track record of using mercenary spyware to target human rights defenders and political opposition, and the UAE has a long and very disturbing history of employing defense and intelligence contractors for information operations."[79] This sends a mixed signal about U.S. policy intent. On the one hand, the Biden administration has admirably cracked down on NSO Group and other firms with unlawful patterns of behavior. Yet, by entering into a cyber agreement with governments that routinely abuse spyware, the administration undercuts its other actions.

When it comes to Israel, accomplishing a major shift on spyware is unlikely. But two small ideas could help. One of the few multilateral configurations designed to address the proliferation of intrusion malware is the Wassenaar Arrangement. While Israel has incorporated the Wassenaar list of dual-use items in its export control regime, it currently is not a formal member of the arrangement and is exempt from reporting on its transactions and full disclosure of its activities in this area.[80] While Wassenaar suffers from its own limitations, such as relying on the voluntary cooperation of its members to enforce compliance, all sides would benefit from Israel officially joining the arrangement.

Second, Israel's licensing regime, overseen by the Ministry of Defense, gives scant consideration to the human rights or democracy records of recipient governments. Israel continues to approve spyware exports to a bevy of authoritarian states. When Israel has denied licenses—such as by excluding Bangladesh from its list of approved countries—this has been done for geopolitical reasons (regarding the export prohibition against Bangladesh, Israel was concerned that sensitive technology would fall into the hands of Pakistan).[81] While it is reasonable for Israel to prioritize its national security, its authorities should also take into account the human rights records of potential recipients. The Israeli government may have little interest in incorporating human rights considerations in its licensing process, but NSO Group's blacklisting offers an opening. In Israel's bid to reverse the U.S. decision, its government offered to implement "much tighter supervision on licensing."[82] The Biden administration should make these trade-offs more explicit: restrict commercial spyware exports to human rights–abusing countries, or other spyware firms will be placed on the Entity List.

The global spyware and digital forensics market continues to expand; governments display an unceasing appetite to acquire intrusive surveillance instruments that are doing irreparable harm to the rights to privacy and freedom of expression and opinion. As digital technology becomes central to economic and political life, it is imperative that citizens demand accountability for these products and that democratic governments respond accordingly.

Appendix I. Global Inventory of Commercial Spyware and Digital Forensics Technology

Note: the complete global spyware and digital forensics inventory can be accessed here: https://data.mendeley.com/datasets/csvhpkt8tm/10. The table below represents a distillation of more comprehensive findings.

Country of deployment	Regime Type	Commercial Entity	Description
Angola	EA	FinFisher	Implicated in targeting of activists
Argentina	ED	Cellebrite	Supplied federal security forces with tools for hacking into locked mobile devices since the early 2010s
Armenia	ED	Cytrox	Purchased by government-backed actors
Azerbaijan	EA	Hacking Team, NSO Group	Evidence indicates that government operators have used surveillance technology to spy on civil society since 2009
Bahrain	CA	Cellebrite, FinFisher, NSO Group	Cellebrite software used to prosecute and torture dissidents; Arab Spring activists hacked
Bangladesh	EA	Cellebrite, FinFisher, NSO Group	Intrusion technology purchased by Bangladesh's Rapid Action Battalion, which has a record of abductions, torture, and disappearances
Belarus	EA	Cellebrite, Grayshift, Oxygen Software	Used intrusion software to hack activists and journalists
Belgium	LD	FinFisher, NSO Group	Belgian Federal Police linked to acquisition of FinFisher and Pegasus spyware

Country of deployment	Regime Type	Commercial Entity	Description
Botswana	LD	AccessData, Cellebrite	Police used software extraction to investigate journalist sources
Brazil	ED	Cellebrite, Hacking Team	History of surveillance abuses; infiltration of online platforms and political monitoring are common
Bulgaria	ED	FinFisher	Identified intrusion server registered to the Bulgarian Ministry of State Administration and Administrative Reform
Canada	LD	Undisclosed	Canadian national police used spyware in ten investigations between 2018 and 2020
Chile	LD	Hacking Team	Investigations Police paid 2.2 million euros to buy RCS Lab spyware
China	CA	Cellebrite, Fiberhome, Meiya Pico, Resonant, Zhongke Ronghui	Xinjiang visitors forced to download Fengcai spyware app; widespread digital forensics use by police
Colombia	ED	AccessData, Cytrox, Hacking Team, Mollitiam	Administrative Department of Security agents used mobile forensic units to obtain private data from devices; conducted surveillance of regime opponents
Côte d'Ivoire	EA	Cytrox	Likely government actor purchased Cytrox exploits
Cyprus	LD	Hacking Team	Head of intelligence service stepped down because of Hacking Team breach
Djibouti	EA	NSO Group	During former president Donald Trump's administration, the U.S. Central Intelligence Agency purchased Pegasus for Djibouti, which used the tool for at least a year
Ecuador	ED	Hacking Team	Leaked documents exposed illegal spying on politicians, journalists, and activists
Egypt	EA	Cytrox, FinFisher, Hacking Team, Meiya Pico, NSO Group	Malware campaigns against civil society
El Salvador	EA	NSO Group	Pegasus spyware used against journalists and activists
Estonia	LD	NSO Group	Israel authorized Estonia to acquire Pegasus in 2018; Estonia made a down payment of $30 million for the system
Ethiopia	EA	Cyberbit, FinFisher, Hacking Team	Targeted Ethiopian dissidents residing in the United States, United Kingdom, and other countries; targeted opposition and civil society in Ethiopia
Gabon	EA	FinFisher	Targeted opposition members and civil society
Germany	LD	Cellebrite, DigiTask, NSO Group	Police unit prosecuting online hate speech can access Cellebrite to break into phones; federal criminal police purchased Pegasus for select antiterrorist and anti–organized crime operations
Ghana	ED	Cellebrite, NSO Group	Possible use against journalists; allegedly planned to use Pegasus to snoop on the opposition ahead of the 2017 election
Greece	LD	Cytrox	Intelligence services used Predator spyware to spy on MEP Androulakis and investigative journalists
Honduras	EA	Cellebrite, Hacking Team	Intrusion technologies acquired by Honduras's police

Country of deployment	Regime Type	Commercial Entity	Description
Hong Kong	CA	Cellebrite, MSAB	Law enforcement in China and Hong Kong continue to acquire Cellebrite's UFED product, allowing officers to break into phones and siphon data
Hungary	EA	Black Cube, Candiru, Hacking Team, NSO Group	Black Cube involved in campaign to discredit nongovernmental organizations ahead of elections; Pegasus used to monitor journalists, media company owners, lawyers, opposition, and government officials
India	EA	Cellebrite, NSO Group	Used spyware to target hundreds of journalists, activists, opposition politicians, government officials, and business executives
Indonesia	ED	Candiru, Cellebrite, Cytrox, FinFisher, NSO Group	Persecuted LGBT population, religious minorities
Israel	LD	NSO Group	Police reportedly used Pegasus against antigovernment protests, senior politicians, mayors, and employees of government-owned companies; Pegasus also found on Palestinian activists' cellphones
Italy	LD	eSurv, FinFisher, Hacking Team, RCS Labs	State police used spyware; concerns that intel agencies are intercepting personal communications employing hacking without statutory authorization or safeguards
Jordan	CA	FinFisher, NSO Group	Used malware to spy on journalists, human rights defenders, and opposition
Kazakhstan	EA	FinFisher, Hacking Team, NSO Group, Oxygen Software, RCS Lab	Obtained software to monitor and interfere with online traffic and perform targeted cyber attacks against users and devices; dozens of government and business persons surveilled
Kenya	EA	FinFisher, NSO Group	Spyware reportedly used to repress civil society organizations and human rights defenders; linked to National Security Intelligence
Lebanon	EA	Dark Caracal, FinFisher, Hacking Team	Developed unique mobile surveillance tool, Dark Caracal/ Pallas, to extract data from Android devices
Madagascar	EA	Cytrox	Likely government-backed actors purchased Cytrox exploits
Malaysia	EA	FinFisher, Hacking Team	Citizen Lab discovered a booby-trapped document that contained a candidate list for 2013 Malaysian general elections
Mexico	ED	FinFisher, Hacking Team, NSO Group, Quadream	Reporters and activists hacked with NSO Group spyware
Mongolia	ED	FinFisher	Linkages between FinFisher malware and State Special Security Department
Morocco	CA	FinFisher, Hacking Team, NSO Group, Cellebrite, MSAB	Supreme Council of National Defense allegedly used spyware; RCS Lab spyware used against Moroccan media outlet Mamfakinch
Myanmar	CA	Cellebrite, MSAB, OpenText, Magnet Forensics, SecurCube, SalvationDATA, EaseUS, iMyFone, Elcomsoft, Silicon Forensics, Sirchie, Passware, Oxygen Software, SysTools	Used Cellebrite to collect data from journalists' smartphones; ordered telecommunications companies to install intercept spyware

Country of deployment	Regime Type	Commercial Entity	Description
Netherlands	LD	DigiTask, NSO Group	DigiTask sold spyware to public authorities; police and security service used Pegasus to track down a crime suspect
Nigeria	EA	Cellebrite, AccessData, Hacking Team, FinFisher	Intrusion software used to spy on politicians and regime opponents; Hacking Team worked with the governor of the state of Bayelsa; Nigerian security forces also purchased spyware
Oman	CA	Hacking Team, FinFisher, Cytrox	Ministry of Interior linked to targeted surveillance
Pakistan	EA	FinFisher	Used malware to infect PowerPoint documents and steal files from targeted computers
Panama	ED	Hacking Team, NSO Group	Ex-president accused of using Pegasus to spy on political enemies, business rivals, and even a mistress; used software to track 150 people illegally
Paraguay	ED	FinFisher	Used spyware on journalists
Philippines	EA	Cytrox, Meiya Pico	Identified as a Cytrox customer
Poland	ED	Hacking Team, NSO Group	Law and Justice party's leader admitted purchasing Pegasus, which was used against various opposition leaders
Romania	ED	FinFisher	Purchase linked to government actors
Russia	EA	Cellebrite, Hacking Team, Meiya Pico	Online accounts of journalists and civil society activists often compromised, indicating a coordinated campaign to access their data
Rwanda	EA	NSO Group	Security officials authorized to tap online communications; Pegasus targeted Rwandan dissidents and Belgian journalists
Saudi Arabia	CA	Hacking Team, NSO Group, FinFisher, Candiru, Cytrox, Quadream, Cellebrite	Extensive documented abuses of spyware to target political opponents and civil society
Serbia	EA	Cytrox, FinFisher	FinFisher use linked to Security Information Agency
Singapore	EA	FinFisher, Quadream, Hacking Team	Legal framework regulating communications interception falls short of international human rights standards; oversight is nonexistent
Slovenia	ED	FinFisher	Identified as a FinFisher client
South Africa	ED	FinFisher	Reportedly conducted surveillance of activists, journalists, and political opponents
Spain	LD	NSO Group, Candiru, Cytrox, Hacking Team	Government targeted Catalan politicians
Sudan	CA	Cytrox, Hacking Team	Allegedly equipped the Rapid Support Forces with sophisticated surveillance technology
Switzerland	LD	DigiTask	DigiTask sold spyware to public authorities in Switzerland
Thailand	CA	Hacking Team, NSO Group	Engaged in targeted surveillance against civil society, regime opponents
Togo	EA	NSO Group	Targeted Togo civil society during nationwide pro-reform protests, which the state forcibly dispersed
Türkiye	EA	Hacking Team, FinFisher, Cellebrite	Taps and intercepts most forms of telecommunication

Country of deployment	Regime Type	Commercial Entity	Description
Turkmenistan	EA	FinFisher	Conducted targeted surveillance against its citizens
Uganda	EA	FinFisher, NSO Group, Cellebrite	Used spyware against opposition leaders, media, and establishment insiders
United Arab Emirates	CA	DarkMatter, Hacking Team, Candiru, FinFisher, NSO Group, Cellebrite	Surveilled newspaper editor; tracked regime opponents
United States	LD	Cellebrite, AccessData, BlackBag, Grayshift, Hacking Team, Magnet Forensics, MSAB, Oxygen Software, Paraben, Paragon, Passware, Elcomsoft, Susteen	Federal Bureau of Investigation (FBI) has purchased at least $2 million worth of Cellebrite products since 2012; FBI, Drug Enforcement Administration, and the U.S. Army implicated in dealings with Hacking Team
Uzbekistan	CA	Hacking Team, Candiru, Oxygen Software, NSO Group	Deployed invasive software to hijack devices
Venezuela	EA	FinFisher, Cellebrite	Conducted widespread targeting of journalists, opposition
Vietnam	CA	FinFisher, Cytrox	Likely government-backed actors purchased exploits
Zambia	EA	NSO Group	Government linked to Pegasus purchase

About the Authors

Steven Feldstein is a senior fellow in the Democracy, Conflict, and Governance Program at the Carnegie Endowment for International Peace. He authored *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (2021), which was the recipient of the 2023 Grawemeyer Award for Ideas Improving World Order.

Brian Kot is a research assistant in the Democracy, Conflict, and Governance Program at the Carnegie Endowment for International Peace.

Notes

1 Dana Priest, Craig Timberg, and Souad Mekhennet, "Private Israeli Spyware Used To Hack Cellphones of Journalists, Activists Worldwide," *Washington Post*, July 18, 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_4.

2 "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," U.S. Department of Commerce, November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list; Davide Scigliuzzo, "Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop," *Bloomberg*, November 22, 2021, https://www.bloomberg.com/news/articles/2021-11-22/israeli-spyware-firm-nso-seen-at-risk-of-default-as-sales-drop?leadSource=uverify%20wall.

3 Hendrik Mildebrath, "Greece's Predatorgate," European Parliamentary Research Service, September 2022, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf.

4 Bill Marczak et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," Citizen Lab, December 16, 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

5 Marczak et al., "Pegasus vs. Predator."

6 Lorenzo Franceschi-Bicchierai, "Hacking Team Founder: 'Hacking Team is Dead,'" Vice, May 26, 2020, https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead.

7 Ryan Gallagher, "Spyware Vendor FinFisher Claims Insolvency Amid Investigation," *Bloomberg*, March 28, 2022, https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation?leadSource=uverify%20wall&sref=QmOxnLFz.

8 Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," *Wired*, July 6, 2015, https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

9 Patrick Howell O'Neill, "The Fall and Rise of a Spyware Empire," *MIT Technology Review*, November 29, 2019, https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/; Joseph Cox and Lorenzo Franceschi-Bicchierai, "Memento Labs, the Reborn Hacking Team, Is Struggling," Vice, March 31, 2020, https://www.vice.com/en/article/xgq3qd/memento-labs-the-reborn-hacking-team-is-struggling.

10 Ronan Farrow, "How Democracies Spy on Their Citizens," *New Yorker*, April 18, 2022, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

11 For purposes of this paper, when the terms "global spyware industry" or "spyware market" are used, the reader should assume this is referring to both spyware products and digital forensics technologies. As explained in the paper, there is a close, overlapping relationship between the two technologies.

12 Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," annual report of the United Nations High Commissioner for Human Rights, A/HRC/51/17, August 4, 2022.

13 Ronald Deibert, "The Autocrat in Your iPhone," *Foreign Affairs*, January/February 2023, https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert.

14 Dana Priest, "A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months Before His Murder, New Forensics Show," *Washington Post*, December 21, 2021, https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/.

15 Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age."

16 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "Surveillance and Human Rights," A/HRC/41/35, May 28, 2019.

17 Report of the Special Rapporteur, "Surveillance and Human Rights."

18 Dunja Mijatović, "Highly Intrusive Spyware Threatens the Essence of Human Rights," Council of Europe Human Rights Comment, January 27, 2023, https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights.

19 Masashi Crete-Nishihata et al., "Communities @ Risk: Targeted Digital Threats Against Civil Society," The Citizen Lab, University of Toronto, 2014, https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

20 Report of the Special Rapporteur, "Surveillance and Human Rights."

21 Steven Feldstein, *Commercial Spyware Global Inventory*, V2 (December 22, 2020), available on Data Mendeley, https://data.mendeley.com/datasets/csvhpkt8tm/2; Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (New York: Oxford University Press, 2021); Steven Feldstein, "Governments Are Using Spyware on Citizens. Can They Be Stopped?," Carnegie Endowment for International Peace, July 21, 2021, https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

22 Steven Feldstein and Brian Kot, *Global Inventory of Commercial Spyware & Digital Forensics*, last updated on January 11, 2023, available via Carnegie Endowment for International Peace, https://carnegieendowment.org/programs/democracy/commercialspyware.

23 Special thanks to Edin Omanovic from Privacy International for additional data collected on global spyware firms.

24 Ryan Gallagher, "'Zero-Click' Hacks Are Growing in Popularity. There's Practically No Way to Stop Them," *Bloomberg*, February 17, 2022, https://www.bloomberg.com/news/articles/2022-02-17/-zero-click-hacks-by-nso-group-and-others-growing-in-popularity.

25 Ben Nimmo and David Agranovich, "Meta's Adversarial Threat Report, Second Quarter 2022," Meta, August 4, 2022, https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.

26 Deibert, "The Autocrat in Your iPhone."

27 Nimmo and Agranovich, "Meta's Adversarial Threat Report."

28 Casey Newton, "Three Wild Stories from Facebook's Counter-Espionage Team," *Platformer*, August 4, 2022, https://www.platformer.news/p/three-wild-stories-from-facebooks. Also of interest: Why would Microsoft-owned Github host malware code in the first place that could be used to unlawfully break into government and activist devices?

29 Lorenzo Franceschi-Bicchierai, "Government Spyware Maker Accidentally Doxes Itself in Amazing Self-Own," Vice, March 17, 2015, https://www.vice.com/en/article/kbyg7a/government-spyware-maker-doxes-itself-by-linking-to-its-site-in-malware-code.

30 Lorenzo Franceschi-Bicchierai, "'Scam' Spyware Vendor Gets Caught, Once Again," Vice, May 19, 2020, https://www.vice.com/en/article/wxq85w/scam-spyware-vendor-gets-caught-once-again.

31 Thomas Brewster, "Meet The 'Cowboys Of Creepware' – Selling Government-Grade Surveillance To Spy On Your Spouse," *Forbes*, February 16, 2017, https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware/?sh=580f17dc455c.

32 Newton, "Three Wild Stories."

33 Sam Sabin, "OpenAI's ChatGPT Previews How AI Can Help Hackers Breach More Networks," *Axios*, January 3, 2022, https://www.axios.com/2023/01/03/hackers-chatgpt-cybercrime-help.

34 Of note, the Wassenaar Arrangement, a group of forty-two advanced economies that coordinates export restrictions for conventional arms and dual-use technology, defines "intrusion software" to include technologies that perform "the extraction of data or information, from a computer or network-capable device, or the modification of system or user data." Thus, phone extraction technologies and spyware would fall into similar categories, as the outcome of using either technology is comparable: hacking or breaching devices containing confidential information in violation of individuals' privacy. See "Wassenaar Arrangement: List of Dual-Use Goods and Technologies and Munitions List," compiled by the Wassenaar Arrangement Secretariat, December 2021, https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-II-2021-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-2021.pdf.

35 "A Technical Look at Phone Extraction," Privacy International, October 14, 2019, https://privacyinternational.org/long-read/3256/technical-look-phone-extraction#:~:text=Upon%20connection%2C%20the%20UFED%20loads,entries%2C%20pictures%2C%20etc.%E2%80%9D.

36 Joseph Cox, "Instructions Show How Cops Use GrayKey to Brute Force iPhones," Vice, June 22, 2021, https://www.vice.com/en/article/k7835w/how-to-brute-force-iphones-graykey.

37 Maximilian Zinkus, Tushar M. Jois, and Matthew Green, "Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," *arXiv*, May 26, 2021, 36, https://arxiv.org/abs/2105.12613.

38 Logan Koepke et al., "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," Upturn, October 20, 2020, https://www.upturn.org/work/mass-extraction/.

39 "Investor Presentation," Cellebrite, August 2021, https://web.archive.org/web/20210829145853/https://sec.report/Document/0001213900-21-042148/.

40 Following the exposure of these problematic business deals and a public pressure campaign, Cellebrite has withdrawn from markets such as Bangladesh, Belarus, China, Hong Kong, Russia, and Venezuela. However, subsequent reports indicate that Cellebrite has failed to completely cut off its ex-customers from its technology. In the case of China, even after Cellebrite claimed to exit the market and deregister its Chinese subsidiary in early 2021, third-party resellers continue to peddle Cellebrite technology to police departments and security agents. Similarly, Cellebrite announced in March 2021 that it would stop selling its products and services to Russia and Belarus. Yet, Russia's main governmental investigative body continues to "actively use" Cellebrite's UFED system. See: Mara Hvistendahl, "Chinese Police Kept Buying Cellebrite Phone Crackers After Company Said It Ended Sales," *Intercept*, August 26, 2021, https://theintercept.com/2021/08/26/cellebrite-china-cellphone-hack/; Oded Yaron, "Russia Still Using Israeli Tech to Hack Detainees' Cellphones," *Haaretz*, October 21, 2022, https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000.

41 Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age."

42 Crofton Black et al., "Revealing Europe's NSO," *Lighthouse Reports*, August 28, 2022, https://www.lighthousereports.nl/investigation/revealing-europes-nso/; Justin Albrecht and Paul Shunk, "Lookout Uncovers Hermit Spyware Deployed in Kazakhstan," Lookout, June 16, 2022, https://www.lookout.com/blog/hermit-spyware-discovery.

43 "Untangling KNOTWEED: European Private-sector Offensive Actor Using 0-day Exploits," Microsoft Threat Intelligence Center and Microsoft Security Response Center, July 27, 2022, https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/.

44 Sophie in't Veld, *Draft Report* (Brussels: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, November 8, 2022), https://www.politico.eu/wp-content/uploads/2022/11/08/PEGA-draft-report-final-8-1117473.pdf.

45 Council Regulation (EC) No 428/2009 of 5 May 2009: Setting Up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items (Recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428.

46 *Operating from the Shadows: Inside NSO Group's Corporate Structure* (London: Amnesty International, Privacy International, and the Centre for Research on Multinational Corporations, 2021), https://www.amnesty.org/en/documents/doc10/4182/2021/en/.

47 Tasos Telloglou et al., "Flight of the Predator," *Lighthouse Reports*, November 30, 2022, https://www.lighthousereports.nl/investigation/flight-of-the-predator/.

48 In't Veld, *Draft Report*.

49 Oded Yaron and Zulkarnain Saer Khan, "Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record," *Haaretz*, January 10, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-01-10/ty-article/.premium/israeli-spy-tech-sold-to-worlds-third-largest-muslim-country/00000185-9692-d16a-a987-f6b75dd00000.

50 *Operating From the Shadows.*

51 *Operating from the Shadows.*

52 *Operating from the Shadows;* Maaike Goslinga, Dimitri Tokmetzis, Sebastian Gjerding, and Lasse Skou Andersen, "How European Spy Technology Falls into the Wrong Hands," *Correspondent,* February 23, 2017, https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153.

53 *Report from the Commission to the European Parliament and the Council on the Implementation of Regulation (EU) 2021/821 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer Of Dual-use Items* (Brussels: European Commission, November 2021), 6, https://trade.ec.europa.eu/doclib/docs/2021/november/tradoc_159936.pdf.

54 Ilia Siatitsa, "Statement before the European Parliament Hearing on 'Spyware Used in Third Countries and Implications for EU Foreign Relations,'" Privacy International, December 14, 2022, https://privacyinternational.org/advocacy/5002/statement-european-parliament-hearing-spyware-used-third-countries-and-implications.

55 Siatitsa, "Statement before the European Parliament."

56 "EU Watchdog Finds Commission Failed to Protect Human Rights From its Surveillance Aid to African Countries," Privacy International, December 5, 2022, https://privacyinternational.org/press-release/4992/eu-watchdog-finds-commission-failed-protect-human-rights-its-surveillance-aid; "Decision on How the European Commission Assessed the Human Rights Impact before Providing Support to African Countries to Develop Surveillance Capabilities (Case 1904/2021/MHZ)," European Ombudsman, decision on November 28, 2022, https://www.ombudsman.europa.eu/en/decision/en/163491.

57 In't Veld, *Draft Report*, 5.

58 Farrow, "How Democracies Spy."

59 John Scott-Railton et al., "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru," Citizen Lab, April 18, 2022, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

60 Deibert, "The Autocrat in Your iPhone."

61 Deibert, "The Autocrat in Your iPhone."

62 Hagar Shezaf and Jonathan Jacobson, "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haaretz*, October 20, 2018, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.

63 Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," *New York Times Magazine*, January 28, 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

64 Gur Megiddo, "'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers," *Haaretz*, December 17, 2021, https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000.

65 Shuki Sadeh, "A Shady Israeli Intel Genius, His Cyber-spy Van and Million-dollar Deals," *Haaretz*, December 31, 2020, https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000.

66 The *New York Times* reports, for example, that the Israeli government "secretly authorized" NSO Group and other cyber espionage companies to continue supplying spying tools to Saudi Arabia, despite public outcry following the murder of Khashoggi. In addition to being a lucrative commercial opportunity, this came at a moment when Israel was reorienting its foreign policy and looking to deepen ties with Persian Gulf countries to counter Iran. Ronen Bergman and Mark Mazzetti, "Israeli Companies Aided Saudi Spying Despite Khashoggi Killing," *New York Times*, July 17, 2021, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html.

67 Craig Timberg et al., "Israel Blocked Ukraine from Getting Potent Pegasus Spyware," *Washington Post*, March 23, 2022, https://www.washingtonpost.com/technology/2022/03/23/urkraine-spyware-pegasus-russia/; Ronen Bergman and Mark Mazzetti, "Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia," *New York Times,* March 23, 2022, https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html.

68 Timberg et al., "Israel Blocked Ukraine."

69 Lawrence Ukenye, Alexander Ward, and Matt Berg, "Why Israel Won't Change Course on Ukraine," *Politico*, January 11, 2023, https://www.politico.com/newsletters/national-security-daily/2023/01/11/why-israel-wont-change-course-on-ukraine-00077408.

70 Ronen Bergman and Patrick Kingsley, "Despite Abuses of NSO Spyware, Israel Will Lobby U.S. to Defend It," *New York Times*, November 8, 2021, https://www.nytimes.com/2021/11/08/world/middleeast/nso-israel-palestinians-spyware.html.

71 Scigliuzzo, ""Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop;" Byron Tau and Dustin Volz, "Head of Israeli Cyber Firm NSO Group Reaffirms Company Commitment to Spyware," *Wall Street Journal*, January 26, 2023, https://www.wsj.com/articles/head-of-israeli-cyber-firm-nso-group-reaffirms-company-commitment-to-spyware-11674738269.

72 Telloglou et al., "Flight of the Predator."

73 in 't Veld, *Draft Report*.

74 in 't Veld, *Draft Report*.

75 Telloglou et al., "Flight of the Predator."

76 Tonya Riley, "White House Expected to Issue Executive Order Reining in Spyware," Cyberscoop, November 18, 2022, https://cyberscoop.com/white-house-spyware-executive-order-himes/.

77 Koepke et al, "Mass Extraction."

78 Tim Starks and Ellen Nakashima, "The Abraham Accords Expand with Cybersecurity Collaboration," *Washington Post*, January 31, 2023, https://www.washingtonpost.com/politics/2023/01/31/abraham-accords-expand-with-cybersecurity-collaboration/.

79 Starks and Nakashima, "The Abraham Accords Expand."

80 Uzi Eilam, "Defense Export Control in 2007: State of Affairs," Institute for National Security Studies, March 2007, https://www.inss.org.il/wp-content/uploads/2022/12/fe-3099671090.pdf; "Israel Export Control Information," Bureau of Industry and Security, U.S. Department of Commerce, accessed January 11, 2023, https://www.bis.doc.gov/index.php/enforcement/220-eco-country-pages/1147-israel-export-control-information.

81 Yaron and Khan, "Israeli Spy Tech Sold to Bangladesh."

82 Bergman and Kingsley, "Despite Abuses of NSO Spyware."

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers around the world. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org