Atlantic Council

CYBER STATECRAFT INITIATIVE

CENTER FOR SECURITY, INNOVATION, AND NEW TECHNOLOGY

Mythical Beasts and Where to Find Them

MAPPING THE GLOBAL SPYWARE MARKET AND ITS THREATS TO NATIONAL SECURITY AND HUMAN RIGHTS

Jen Roberts, Trey Herr, Nitansha Bansal, and Nancy Messieh with Emma Taylor, Jean Le Roux and Sopo Gelava

Atlantic Council

CYBER STATECRAFT INITIATIVE

CENTER FOR SECURITY, INNOVATION, AND NEW TECHNOLOGY

The Cyber Statecraft Initiative, part of the ACTech programs, works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The Center for Security, Innovation and New Technology is an interdisciplinary program committed to advancing research and policy on the security and power dilemmas stemming from digital and emerging technologies. Based at the School of International Service at American University, our faculty and students work on issues such as interstate cyber conflict, the proliferation and mitigation of spyware, disinformation and foreign influence operations, and the geopolitics of frontier technologies. We combine technical analysis with social science frameworks to contextualize contemporary policy debates about the challenges and opportunities of digital and emerging technologies.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

September 2024

ISBN is 978-1-61977-348-6

Design by: Donald Partyka

Illustrations: Andrey Prokopenko

Atlantic Council
CYBER STATECRAFT INITIATIVE
CENTER FOR SECURITY, INNOVATION, AND NEW TECHNOLOGY

Mythical Beasts and Where to Find Them

MAPPING THE GLOBAL SPYWARE MARKET AND ITS THREATS TO NATIONAL SECURITY AND HUMAN RIGHTS

Jen Roberts, Trey Herr, Nitansha Bansal, and Nancy Messieh with Emma Taylor, Jean Le Roux and Sopo Gelava

TABLE OF CONTENTS

Executive Summary 1

Introduction 2

- Briefly Through the Past
- More Recently
- A Turn to the Spyware Market

Methods, Definitions, and Navigating this Dataset 7

- ...so “Commercial” Spyware?
- A Final Note on Scope
- Building the Dataset
- Defining Entities in the Spyware Market

Analysis 10

1. The Three I’s
2. Serial Entrepreneurs
3. Partnerships with Hardware Surveillance
4. Shifting Vendor Identities
5. Strategic Jurisdiction Hopping
6. Money From Across the World Fuels the Spyware Market

Policy Recommendations 22

- Mandate “Know Your Vendor” requirements
- Improve government-run corporate registries
  - 2.1 Expand the minimum scope of data captured by registries
  - 2.2 Expand beneficial ownership identification
  - 2.3 Make government-run corporate registry data public
- Enrich, audit, and publish export licenses
- Limit jurisdictional arbitrage by vendors
- Provide greater protection against Strategic Lawsuits Against Public Participation (SLAPP)

Areas for Future Work and Conclusion 29

- Future Work

Conclusion 31

Acknowledgments 31

Appendices 32

- Appendix A — Supplier and Vendor Profiles
  - Suppliers
  - Vendors
- Appendix B — Markets Map: Country list (42)
- Appendix C — Markets Map: Vendor List (49)

About the authors 42

EXECUTIVE SUMMARY

Despite its contribution to human rights harms and national security risks, the proliferation of spyware remains rife. A significant channel for this proliferation is sale through a global market, of which most public information is known about only a handful of vendors. While some of these entities have achieved infamy, like NSO Group and the Intellexa Consortium, most others have largely flown under the radar.

The Mythical Beasts project addresses this meaningful gap in contemporary public analysis on spyware proliferation, pulling back the curtain on the connections between 435 entities across forty-two countries in the global spyware market. These vendors exist in a web of relationships with investors, holding companies, partners, and individuals often domiciled in different jurisdictions.

This market is a significant vector for facilitating the human rights harms and national security risks posed more broadly by spyware, software that facilitates unauthorized remote access to internet-enabled target devices for purposes of surveillance or data extraction. It is possible for policymakers to make significant progress in limiting these harms and risks by influencing this market, rather than playing "whack-a-mole" with individual vendors or transactions. This progress is possible now, even in the face of basic disagreements over what constitutes a "legitimate" use of spyware. Besides changes to participants in the market, greater transparency will also support more effective policies related to spyware, rooted in cooperative international action.

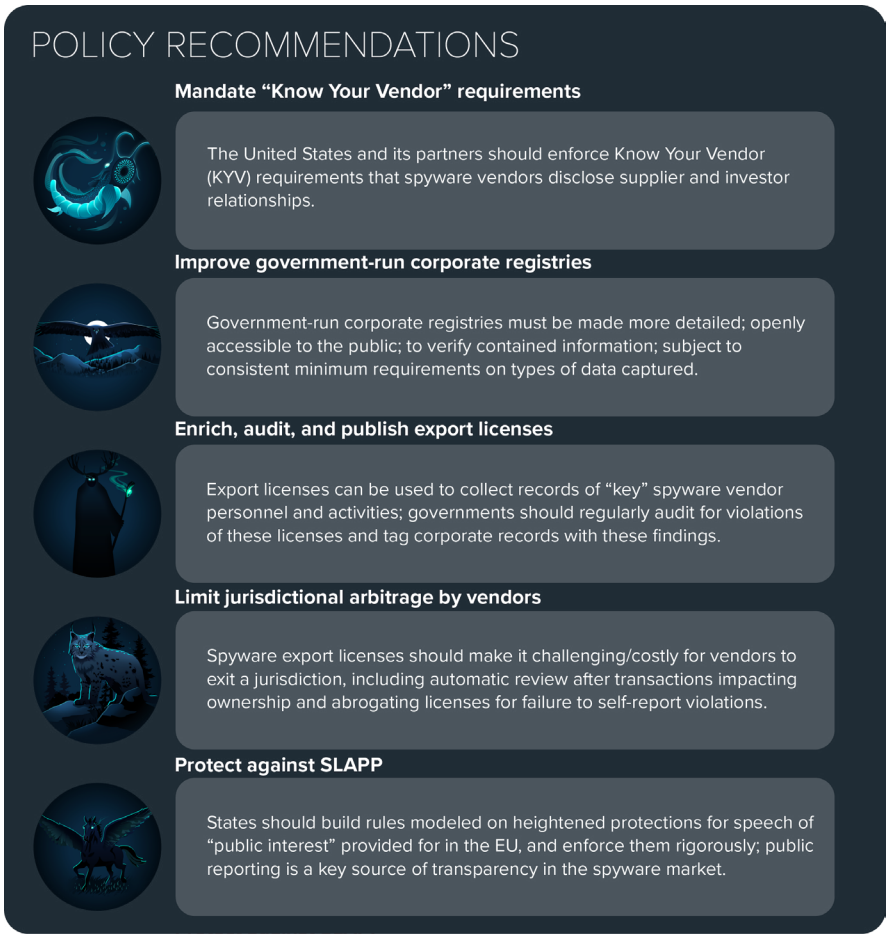

FIGURE 1: Policy recommendations to produce greater transparency across the market

Developed as part of a wider study of proliferation and international cybersecurity, this report provides an analysis of the accompanying dataset comprised of information from 1992 to 2023 on forty-nine vendors along with thirty-six subsidiaries, twenty-four partner firms, twenty suppliers, and a mix of thirty-two holding companies, ninety-five investors, and one hundred and seventy-nine individuals, including many named investors. There are six trends that hold for this dataset, a detailed but even still incomplete sample: 1) concentration of entities in three major jurisdictions (Israel, Italy, and India), 2) serial entrepreneurship across multiple vendors, 3) partnerships between spyware and hardware surveillance vendors, 4) regularly shifting vendor identities, 5) strategic jurisdiction hopping, and 6) cross-border capital flows fueling this market.

These trends inform a set of policy recommendations to produce greater transparency across the market, limit the jurisdictional arbitrage of vendors seeking to evade limits on their behavior, and more effectively scrutinize supplier and investor relationships.

Commercial acquisition of spyware is not the root cause of its abuse. While this project is focused on bringing transparency to participants in this market, it does not argue that only transactions through this market pose proliferation harms or risks. An information gap exists in what is known about the spyware market and its varied participants, a gap that is impeding international cooperation on policies that could meaningfully reduce the harms and risks posed by spyware. This report seeks to offer new data and analysis to bridge that gap and support the work of researchers and policymakers more widely.

INTRODUCTION

For at least the last thirty years, "mythical beasts" have been lurking around the globe, assuming the names of varying species of fish, fowl, and other creatures rooted in lore. These mythical beasts—often with dramatic naming conventions—are spyware: software that facilitates unauthorized remote access to an internet-enabled target device for purposes of surveillance or data extraction. The companies that sell these tools are sustained by an increasingly diverse array of government customers across a global market, even in the face of scattered regulatory efforts targeting spyware supply chains.[1] What is known about this market?

- Out of 195 countries in the world, at least eighty are known to have procured spyware from commercial vendors.[2]
- Fourteen of the twenty-seven countries in the European Union have purchased spyware from just one vendor, the NSO Group.[3]
- Spyware vendors were attributed to fifty percent of all zero-day exploits discovered by one company's threat research team in 2023, including sixty-four percent of all exploits in mobile and browser software.[4]
- While the annual revenue generated by this market is unknown and subject to repeated speculation, largely recycling the same unsourced statistic, at least one vendor has considered an initial public offering valuation of $2 billion.[5]

With the proliferation of spyware, from NSO Group's Pegasus to Intellexa Consortium's Predator, comes increased attention to its use. Some argue that spyware can be employed as a legitimate law enforcement and intelligence tool.[6] It has also been used by states to extend surveillance power well beyond their physical borders, making it easier to track, arrest, kidnap, and even kill their citizens.[7] In these abuses of spyware, the victims are most often journalists, activists, opposition politicians, and a myriad of other individuals whose activity has attracted hostile interest from their governments. For years, civil society organizations like AccessNow and Amnesty International have sought to bring attention to these abuses and have reported on spyware's use on nearly every continent.[8]

State surveillance, harassment, repression, and outright murder predate spyware, and there is little to suggest spyware "causes" these abuses. Measuring the human rights

1 Lorenzo Franceschi-Bicchierai, "Price of Zero-Day Exploits Rises as Companies Harden Products against Hackers," TechCrunch, April 6, 2024, https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/.

2 Alexander Martin, "More than 80 Countries Have Purchased Spyware, British Cyber Agency Warns," The Record, April 19, 2023, https://therecord.media/spyware-purchased-by-eighty-countries-gchq-warns.

3 Pieter Omtzigt, "Pegasus and Similar Spyware and Secret State Surveillance," (Parliamentary Assembly, Council of Europe, September 20, 2023), https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68. See also Jen Roberts et al., "Markets Matter: A Glance into the Spyware Industry," DFRLab, April 22, 2024, https://dfrlab.org/2024/04/22/markets-matter-a-glance-into-the-spyware-industry/.

4 "We're all in this together: A year in review of zero-days exploited in-the-wild in 2023," *Google,* March 2024, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf; Google notes that while the spyware they captured targeted mobile and browser software exclusively, "we know that Candiru Ltd, a CSV, had a chain for Windows because we were able to recover their first stage Chrome exploit, but we were not able to recover the rest of the exploits in the chain."

5 Revenue generated by these sales is difficult to estimate and a subject for further study to include customers and not just the sales side of this market. One widely cited estimate, $12 billion, does not seem to have a rigorous source but is quoted by entities like the Centre for International Governance and Innovation (Kyle Hiebert, "The Growing Global Spyware Industry Must Be Reined In," Centre for International Governance Innovation, March 27, 2023, https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/) and the Carnegie Endowment (Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," March 14, 2023, https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en), as well as a host of media (e.g., Jessica Lyons, "Spyware Business Booming despite Government Crackdowns," *The Register*, February 7, 2024, https://www.theregister.com/2024/02/07/spyware_business_booming/ and Ronan Farrow, "How Democracies Spy on Their Citizens," *The New Yorker*, April 18, 2022, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens). It first appeared in a 2019 *New York Times* article (Mark Mazzetti et al., "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments," *New York Times*, March 21, 2019, https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html)—without citation to a specific source or substantiation. An earlier $5 billion estimate appears in a 2016 Vanity Fair piece by Bryan Burrough attributed to an anonymous expert. Firm Valuation – Reuters, "Israeli cyber firm NSO Group mulls Tel Aviv IPO at $2 billion value – reports", January 6, 2021, accessed July 16, 2024, https://www.reuters.com/article/israel-cyber-nso-ipo-int-idUSKBN29B0WU/.

6 Mike Sexton, "Unregulated Spyware's Threat to National Security – Third Way," June 22, 2023, accessed July 10, 2024, https://www.thirdway.org/memo/unregulated-spywares-threat-to-national-security; US Department of State, "Guiding Principles on Government Use of Surveillance Technology," March 30, 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.

7 Mike Sexton, "Unregulated Spyware's Threat to National Security," Third Way, June 22, 2023, https://www.thirdway.org/memo/unregulated-spywares-threat-to-national-security; A.J. Vicens, "Phones of Journalists and Activists in Europe Targeted with Pegasus," *CyberScoop* (blog), May 30, 2024, https://cyberscoop.com/spyware-europe-nso-pegasus/; Natalie Kitroeff and Ronen Bergman, "How Mexico Became the Biggest User of the Pegasus Spyware," *New York Times*, April 18, 2023, https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html; Fanny Potkin and Poppy McPherson, "Israel's Cognyte Won Tender to Sell Intercept Spyware to Myanmar before Coup," *Reuters,* January 18, 2023, https://www.reuters.com/technology/israels-cognyte-won-tender-sell-intercept-spyware-myanmar-before-coup-documents-2023-01-15/; Siena Anstis et al., *The Dangerous Effects of Unregulated Commercial Spyware*, The Citizen Lab (Munk School, University of Toronto), June 24, 2019, https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/.

8 "Standing Up to Surveillance," AccessNow (blog), accessed July 3, 2024, https://www.accessnow.org/surveillance/; "The Predator Files: Caught in the Net, the Global Threat from 'EU Regulated' Spyware," Amnesty International, October 9, 2023, https://www.amnesty-international.be/sites/default/files/2023-10/act1072452023english.pdf; Bill Marczak et al., *Hooking Candiru Ltd*, Citizen Lab (Munk School, University of Toronto), July 15, 2021, https://citizenlab.ca/2021/07/hooking-Candiru Ltd-another-mercenary-spyware-vendor-comes-into-focus/.

harms and national security risks of spyware against its value to law enforcement or intelligence activities is also challenging as these activities are, by their nature, even less visible. Few governments have sought to demonstrate the range of legitimate uses of spyware or its impacts. As a result, when considering spyware's effects on society, there is a bias to what is known.

Still, what *is* known is an abundance of public evidence of the totality of abuses made easier—perhaps even directly possible—by spyware.[9]

It is not in dispute that spyware makes it easier for states to penetrate even the most robust commercial technologies, cell phones, computers, and communications services; makes it far easier to act against citizens beyond state borders; and even provides governments with the ability to target senior officials, both domestically and abroad, where they might otherwise have no means to do so.[10] Where that information is used to facilitate repression and abuse, its harms are untenable. Where that information is gathered and used subject to due diligence and effective oversight in pursuit of credible law enforcement and intelligence activities subject to the limits of the law, its effects may provide for the public interest. These two categories overlap and are altogether too often separated by good intent and cursory legal review.

The proliferation of spyware also poses national security risks as it makes it more likely for states to become "more capable—for instance while conducting cyber-espionage for commercial or intelligence gain—or ready for more disruptive or damaging operations."[11] The proliferation of these capabilities in most states takes place with few effective restraints, strict controls, or meaningful oversight mechanisms. This is a recognized policy challenge and one which has been taken up in various forms by some governments, largely in Europe, the US, and the UK.

Briefly Through the Past

Digital surveillance technologies, which include spyware, are known as dual-use goods, meaning they can be "used for both defense and civilian purposes."[12] Dual-use technology in forty-two countries falls under a multilateral export control regime established in 1996, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (the Wassenaar Arrangement).[13] In 2013, the Wassenaar Arrangement was amended to include "intrusion software" but after considerable feedback from the security research community and significant delay, the language was revised.[14] While the Wassenaar Arrangement is not legally binding, its signatories typically voluntarily implement its control list into domestic regulations, oftentimes requiring firms whose products are listed to acquire special licenses to export these items.

Within the European Union, export controls are governed by the EU's Dual-Use Regulation.[15] The first EU legislation on dual-use goods was enacted in 1994, underwent significant changes in 2009, and a new version was enacted in 2021 to implement and modernize the EU's export control regime.[16] Member states are required to abide by this common set of restrictions but may introduce additional controls on non-listed dual-use items due to public security or human rights considerations.

The United States is also a participant in the Wassenaar Arrangement and the Bureau of Industry and Security (BIS)

9 As analysis from the Atlantic Council has argued previously, proliferation "presents an expanding set of risks to states and challenges commitments to protect openness, security, and stability in cyberspace. The profusion of commercial offensive cyber capabilities (OCC) vendors, left unregulated and ill-observed, poses national security and human rights risks. For states that have strong OCC programs, the proliferation of spyware to state adversaries or certain non-state actors can be a threat to immediate security interests, long-term intelligence advantage, and the feasibility of mounting an effective defense on behalf of less capable private companies and vulnerable populations. The acquisition of OCC by a current or potential adversary makes them more capable." Winnona DeSombre et al, "Countering Cyber Proliferation: Zeroing in on Access-as-a-Service," *Atlantic Council* (blog), March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

10 Andy Greenberg and Lily Hay Newman, "Security News This Week: US Congress Targeted with Predator Spyware," *Wired,* October 14, 2023, https://www.wired.com/story/us-congress-spyware/; Gordon Corera, "Pegasus: French President Macron Identified as Spyware Target," *BBC,* July 20, 2021, https://www.bbc.com/news/world-europe-57907258.

11 Winnona DeSombre et al., *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service*, Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

12 "Exporting Dual-Use Items," European Commission, accessed July 10, 2024, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.

13 "The Wassenaar Arrangement at a Glance," Arms Control Association, February 2022 [last reviewed], https://www.armscontrol.org/factsheets/wassenaar.

14 "2013 Amendments to Wassenaar Arrangement Need Rewording, US State Dept. Concedes," The Wire, accessed July 10, 2024, https://thewire.in/tech/2013-amendments-to-wassenaar-arrangement-need-rewording-us-state-department-concedes; Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," *Lawfare,* January 5, 2018, https://www.lawfaremedia.org/article/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

15 "Exporting Dual-Use Items," European Commission.

16 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:32009R0428; 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:32009R0428.; "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items (Recast)" (Official Journal of the European Union, June 11, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN.; Mark Bromley and Kolja Brockman, "Implementing the 2021 Recast of the EU Dual-Use Regulation: Challenges and Opportunities," *Eu Non-Proliferation and Disarmament Consortium,* Non-Proliferation and Disarmament Papers, No.77, September 2021, https://www.sipri.org/sites/default/files/2021-09/eunpdc_no_77.pdf.

within the Department of Commerce has the authority to regulate dual-use exports by issuing export licenses.[17] The BIS Entity List contains names and organizations subject to specific additional license requirements.[18] In 2021, BIS added four entities to this list, including for the first time two spyware vendors:

- Candiru Ltd
- NSO Group

And two suppliers:

- COSEINC
- Positive Technologies AO.[19]

In 2023, BIS also added four companies associated with the Intellexa Consortium to the Entity List: Intellexa S.A., Cytrox AD Holdings ZRT, Intellexa Limited (Ireland), and Cytrox AD (North Macedonia) as they were determined by BIS to be "trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide."[20]

In addition to export controls, the European Union and the United States have sought to implement other measures to limit spyware proliferation. In 2022, in response to the investigative findings of the Pegasus Project, an international investigative journalism initiative, the European Parliament established the PEGA Committee to investigate the misuse of surveillance spyware, including the NSO Group's Pegasus and similar spyware services.[21] The committee concluded that European Union governments abused spyware services, lacked necessary safeguards to prevent misuse, and in at least one jurisdiction, Greece, the government had facilitated the export of Predator spyware which was then itself abused, here by Sudan's Rapid Support Forces militias, who are reported to have committed war crimes.[22] Despite the committee's recommendations, the EU has not adopted any legislation as a bloc to curb the development or sale of spyware.[23]

More Recently

The last twenty-one months saw a surge in policymaking activity building on these recent efforts. Most visible has been from the United States, which has enacted punitive measures targeting entities selling spyware and driven some measure of diplomatic consensus to "recognize the threat posed by the misuse of commercial spyware" and acknowledge the "fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware."[24]

In March 2023, the United States first proposed blocking US government agencies from using "commercial spyware." Under Executive Order 14093, the Biden administration prohibited the operational use of commercial spyware that presents a significant threat to national security.[25] Also in March of 2023, the US and several other countries signed The Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, pledging to "work collectively to counter the proliferation and misuse of commercial spyware."[26]

17 Bureau of Industry and Security, U.S. Department of the Commerce, https://www.bis.doc.gov/index.php/91-dual-use-export-licenses; Governed by the Export Administration Regulations.

18 15 C.F.R. § 744, "Control Policy: End-User and End-Use Based," https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744.

19 US Department of State, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities," media note (Office of the Spokesperson), November 3, 2021, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/. Positive and COSEINC were both added, "based on a determination that they misuse and traffic cyber tools that are used to gain unauthorized access to information systems in ways that are contrary to the national security or foreign policy of the United States, threatening the privacy and security of individuals and organizations worldwide."

20 Office of Congressional and Public Affairs, "Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits," press release, US Department of Commerce: Bureau of Industry and Security, July 18, 2023, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3297-2023-07-18-bis-press-package-spyware-document/file.

21 "About the Pegasus Project," *Forbidden Stories,* July 18, 2021, https://forbiddenstories.org/about-the-pegasus-project/; Sophie in 't Veld, "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (Report – A9-0189/2023)," European Parliament, May 5, 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html; European Parliament, 2022/2077(INI), Legislative Observatory, accessed July 10, 2024, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/2077(INI).

22 in 't Veld, "Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI))."; "Sudan: One Year of Atrocities Requires New Global Approach," *Human Rights Watch,* April 12, 2024, https://www.hrw.org/news/2024/04/12/sudan-one-year-atrocities-requires-new-global-approach.

23 Max Griera, "EU Parliament Vote on Spyware Gets Politicised, Implementation Challenges Loom," *Euractiv*, May 9, 2023, https://www.euractiv.com/section/politics/news/eu-parliament-vote-on-spyware-gets-politicised-implementation-challenges-loom/.

24 "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," The White House, March 18, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/; President Biden, "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," press release, The White House, March 27, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.

25 "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security."

26 The White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse."; Even the Summit for Democracy statement points to an admittedly limited statement of "Guiding Principles on Government Use of Surveillance Technologies" which emphasizes it is a "voluntary and non-legally binding" document and calls for actions like, "Governments should ensure the operation of surveillance technologies is governed in a manner that proactively mitigates the risks of misuse and enables appropriate access to judicial or administrative review." While this is a positive starting point, it does not, yet present an implementable model of transparent and rigorous governance of the use of spyware.

In March 2024, the US Department of Treasury Office of Foreign Assets Control levied sanctions against several entities, some of which are also listed on the BIS Entity List.[27] Ultimately Treasury sanctioned:

- Tal Dilian
- Sara Hamou
- Intellexa S.A.
- Intellexa Limited
- Cytrox AD
- Cytrox Holdings Crt
- Thalestris Limited[28]

So far, the US has refrained from sanctioning five other entities within the Intellexa Group, previously identified publicly, and perhaps others, including entities associated with Thalestris Limited.[29] That same month, several additional countries joined as signatories in an expansion of The Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware.[30]

In April 2024, the US Department of State announced a visa restriction policy to "promote accountability for the misuse of commercial spyware."[31] This extended statutory language from 2021, originally implemented as visa bans on "individuals who, acting on behalf of a foreign government, are believed to have been directly engaged in serious, extraterritorial counter-dissident activities, including those that suppress, harass, surveil, threaten, or harm journalists, activists, or other persons perceived to be dissidents for their work, or who engage in such activities with respect to the families or other close associates of such persons."[32] The new restrictions pertain to individuals who have been involved in the development and sale of commercial spyware and their immediate family members.[33] Thirteen individuals, whose identities are not public, have been subject to this action as of the date of this writing.[34]

A new multilateral effort from the UK and French governments, the Pall Mall process, has also brought together an even wider array of state and non-state participants to develop principles, and perhaps practical policy action, to counter spyware proliferation.[35] Pall Mall includes non-state groups and a much wider set of states than the Joint Statement signatories but, so far, with much more ambiguous outcomes, including a debated set of principles and plans for a broad consultative process.

Collectively these US and allied efforts demonstrate there is a growing focus on curtailing the proliferation of spyware. However, still missing from these discussions is a common picture of the spyware market with sufficient detail to understand the diversity of market participants and relationships that stretch across borders.

A Turn to the Spyware Market

This report offers a new dataset covering 435 entities (incl. forty-nine vendors and twenty suppliers) across the spyware market. The data spans forty-two different countries and nearly thirty years, covering vendors, investors, and other corporate relationships. The collection of this data and its publication is an attempt to address a systematic bias toward the operations of a small handful of well-known firms that inform assumptions about the interactions and relationships of a large global market.

This narrow focus has helped obscure the impact of dozens of other vendors and the importance of their relationships with both investors and suppliers of crucial software components, including working exploits of some of the most widely used software (e.g. iOS, Android). This project supports the "turn to spyware" in recent transatlantic policy activity and should enable a more robust, market-first (rather than vendor-centric) approach. Such an approach can leverage both conventional tools to constrain and shape markets as well as new policies to address the unique dimensions of spyware.

27 US Department of the Treasury, "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," press release, March 5, 2024, https://home.treasury.gov/news/press-releases/jy2155. These sanctions were issued pursuant to Executive Order 13694, as amended by Executive Order 13757.

28 US Department of the Treasury, "Treasury Sanctions Members of the Intellexa."

29 Balinese Ltd (formerly Cytrox AD Software Ltd), Peterbald Ltd (formerly Cytrox AD EMEA Ltd), Passitora Ltd (formerly WS WiSpear Systems Limited), and Senpai Technologies Ltd—all currently based in Israel—as well as the British Virgin Islands-domiciled Intellexa Limited.

30 A number of the concepts, some language, and three signatories (Australia, Denmark, and Norway) for this document originated in the first Summit for Democracy as part of the "Export Controls and Human Rights Initiative" – "Fact Sheet: Export Controls and Human Rights Initiative Launched at Summit For Democracy," *The White House,* December 10, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/.

31 "Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware," *U.S. Department of State,* February 5, 2024, https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/.

32 "Accountability for the Murder of Jamal Khashoggi," *U.S. Department of State,* February 26, 2021, https://www.state.gov/accountability-for-the-murder-of-jamal-khashoggi/.

33 Based on authority from Section 212(a)(3)(C) of the Immigration and National Act.

34 "Promoting Accountability for the Misuse of Commercial Spyware," *U.S. Department of State,* April 22, 2024, https://www.state.gov/promoting-accountability-for-the-misuse-of-commercial-spyware/.

35 "The Pall Mall Process Declaration: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities," UK Foreign, Commonwealth & Development Office, February 6, 2024, https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

Unlike other more tightly regulated markets, the market for spyware lacks public data that is consistent, reliable, and clearly sourced. While a single export authority, such as Israel's Defense Exports Control Agency, may track sales out of the country, this information is neither public nor combined with similar resources from other jurisdictions. Thus, the view of the spyware market is limited even for exceptionally well-equipped states. Researchers, journalists, and policymakers alike must scrape through a variety of different resources just to scratch the surface of this market that has cloaked itself in secrecy, making it difficult for policy action. There is some comparison even to be had with the approach of US policymakers in regulating the market for cannabis over the last several decades. Once a widely banned yet still pervasively acquired substance, the cannabis market has now been legalized in many states and is subject to enormous scrutiny. This new approach focused not on blocking cannabis transactions or consumption but rather on leveraging market forces, accepting some legitimate use, and creating parameters for responsible procurement. Proliferation will not be prevented by a well-regulated and more transparent market, but it can be better channeled and made subject to controls, less opaque, and less harmful.

Policy responses to address spyware as a market is preferable over advocacy for a complete ban. Such a ban would likely supercharge government calls for exceptional access to encrypted services and data while sapping momentum toward better approaches to spyware in the US and UK, home to two of the most active policymaking communities on this issue.

An important caveat: the dataset collected here does not catalog use, so the authors cannot make novel claims about what constitutes "legitimate use" of spyware. Few of the policies mentioned in the previous section define legitimate use with sufficient precision to enforce granular bans on behavior and even these are not transparent.[36] The lack of a common understanding of the scale, diversity, and relationships within the spyware market is a barrier to effective policymaking. Thus, this report argues for how to improve transparency in the market and develop sufficient granular controls to enable these kinds of distinctions in use.

The next section of this report explains the methodology associated with this dataset as well as definitions and a summary of the data. The following section analyzes major trends from this data and highlights specific examples and implications for policy before developing specific recommendations. As the authors have written previously, "markets matter," and this report argues that the current surge in policymaking toward spyware can best be sustained and made more impactful by focusing policymaking on the spyware market instead of just a handful of the most well-known firms.[37]

36 Secretary Blinken, "Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware," press statement, United States Department of State, February 5, 2024, https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/.

37 Jen Roberts, Trey Herr, Emma Taylor, and Nitansha Bansal, "Markets Matter: A Glance into the Spyware Industry, *DFRLab,* April 22, 2024, https://dfrlab.org/2024/04/22/markets-matter-a-glance-into-the-spyware-industry/.

METHODS, DEFINITIONS, AND NAVIGATING THIS DATASET

This section discusses the project's scope, including a working definition of spyware, data collection methodology, and sources, and closes with the major definitions and terms used as part of this dataset's coding framework.

Spyware is a type of malicious software that facilitates unauthorized remote access to an internet-enabled target device for purposes of surveillance or data extraction.[38] Spyware is sometimes referred to as "commercial intrusion [or] surveillance software" with effectively the same meaning.[39] This research considers the "tools, vulnerabilities, and skills, including technical, organizational, and individual capacities" as part of the supply chain for spyware and the meaningful risks posed by the proliferation of many of these components.[40]

This project is concerned with the commercial market for spyware and provides data on market participants. Focusing on the market does not presume that all harms from spyware stem from how it is acquired, or whether that acquisition is a commercial transaction with a third party (versus developed "in-house" by the customer). Some definitions of spyware differentiate it by the means with which it is acquired, creating confusion over the fundamental distinction between "spyware" and, for instance, "commercial spyware."[41]

...so "Commercial" Spyware?

Transactions across the spyware market may be less regulated than in-house development of spyware but they are far from the only source of harm and insecurity. Policies that seek only to mitigate harms from the commercial sale of these capabilities risk ignoring their wider harms and avoid the opportunity to address fundamental concerns over surveillance and the full spectrum of government uses of these technologies.

The debate over what constitutes legitimate uses of spyware is ongoing, but commercial sale is a poor proxy for the degree of responsible or mature use. History has shown that this market is only one, albeit significant, part of a wider proliferation challenge.[42] Many human rights violations associated with spyware occur in the context of their use for state security purposes (e.g., by intelligence agencies), highlighting the diverse harms and risks posed by the proliferation of spyware. These include what some researchers have termed "vertical" uses (by states against their own populations) and "diagonal" uses (against the population of other states, including diaspora).[43] There is some normative loading in the term "spyware" vs. the more functional "malware" or the rather impenetrable "commercial intrusion capabilities" but is beneficial to have a common term of art in many of these debates.

This report and accompanying dataset are mainly inclusive of investigations into vendors and suppliers that have been found selling spyware to governments across the world that have then used this software to abuse human rights. However, this is only one side of the coin. Far less data exists on the use of spyware for a myriad of intelligence and counterintelligence purposes, including "national security" missions both genuine and troubling. The report cannot resolve these tensions but does seek to frame them in service of a more immediate and practical purpose—and a better understanding of the market that provides the software tools and services to carry out these acts.

38 "Unauthorized" access separates spyware from myriad other services or tools that might be used to effectuate similar surveillance but which require a user's consent at some stage e.g. downloading an application from a mobile phone app store.

39 50 U.S. Code § 3232a - Measures to mitigate counterintelligence threats from proliferation and use of foreign commercial spyware, https://www.law.cornell.edu/uscode/text/50/3232a.

40 Winnona DeSombre et al., "A Primer on the Proliferation of Offensive Cyber Capabilities" (Atlantic Council, March 1, 2021), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

41 "Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security," Federal Register, March 30, 2023, https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to.

42 Read more about the 'breakout' of "offensive capabilities like EternalBlue, allegedly engineered by the United States, used by Russian, North Korean, and Chinese governments" (DeSombre et al., *Countering Cyber Proliferation*). See also Gil Baram, "The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat," Council on Foreign Relations (blog), June 19, 2018, https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat; Insikt Group, "Chinese and Russian Cyber Communities Dig Into Malware From April Shadow Brokers Release," Recorded Future (blog), April 25, 2017, https://www.recordedfuture.com/shadow-brokers-malware-release/; Leo Varela, "EternalBlue: Metasploit Module for MS17-010," Rapid7, May 19, 2017, https://blog.rapid7.com/2017/05/20/metasploit-the-power-of-the-community-and-eternalblue/.

43 Herb Lin and Joel P. Trachtman, "Using International Export Controls to Bolster Cyber Defenses," Protecting Civilian Institutions and Infrastructure from Cyber Operations: Designing International Law and Organizations, Center for International Law and Governance, Tufts University, September 10, 2018, https://sites.tufts.edu/cilg/files/2018/09/exportcontrolsdraftsm.pdf.

Commercial acquisition of spyware is not the root cause of its abuse. While this project is focused on bringing transparency to participants in the spyware market, it does not argue that only transactions through this market pose proliferation risks or harms.[44] To avoid further confusion in both analysis and policy, the authors do not include the term "commercial" in the definition of spyware. While the debate continues about how to manage these risks, this project sheds better light on those buying, selling, and supporting this market.

A Final Note on Scope

Spyware works without the consent or knowledge of the target or others with access to the target's device; thus, this report does not consider the market for so-called "stalkerware," which generally requires physical interaction from an individual, most often a spouse or partner, with access to a user's device.[45] This definition also excludes software that never gains access to a target device, such as surveillance technologies that collect information on data moving between devices over wired (i.e., packet inspection or "sniffing") or wireless connections. This definition also excludes hardware such as mobile intercept devices, known as IMSI catchers, and any product requiring close or physical access to a target device, such as forensic tools.[46]

This definition is limited, by design, to disentangle lumping various other surveillance toolsets into the definition of spyware.

Building the Dataset

This dataset represents a meaningful sample of the market for spyware vendors, but it is not a complete record and this report can only speak to trends and patterns within this data, not the market as a whole. The data is confined to entities for which there is a public record (i.e. registered businesses) and for which public information links the vendor to the development or sale of spyware or its components.[47]

To develop a list of vendors, the authors started by creating an initial "most visible" list of those with the widest public exposure from the use of their wares, relying principally on public reporting from Amnesty International, Citizen Lab, and the Carnegie Endowment for International Peace, as well as public reporting from a variety of news outlets. This initial set of vendors was the starting point for searching public corporate registries and a mix of public and private-sector corporate databases to profile each company in greater depth and find additional connections.

All the vendors identified through this process were included if they 1) publicly advertised products or services that matched the above definition of spyware, 2) were described as selling the same products by public reporting in the media or by civil society researchers, or 3) showed evidence of the products through court records, leaks, or similar internal documentation. As part of this search process, the team gathered records on subsidiaries and branches associated with each vendor, their publicly disclosed investors, and, where possible, named suppliers.

Each entity identified in this process was identified by at least two different open sources. In all cases for which data is available, the dataset includes vendor activities from the start of operation until 2023, or until records indicate that the vendor's registration had ceased in a jurisdiction. The sources of public information on both firms' activities and their organization varied but largely stemmed from different forms of corporate registration, records, and transaction data.

Defining Entities in the Spyware Market

The dataset covers 435 entities present in the spyware market between 1992 and 2023. These entities include vendors along with their branches and subsidiaries, some senior company employees, and a small number of suppliers and partners, as well as investors and holding companies to shed transparency on supply chains that comprise the spyware market. These definitions cover key terms in this project as a way of scoping the analysis. Policymaking around spyware has suffered in the past in part due to unclear terminology and inconsistent definitions. Recognizing the significant energy across ongoing international policymaking efforts on spyware, this section seeks to specify terms of the ongoing debate.

Vendor: A spyware vendor is a commercial entity that develops, supports, and sells spyware to an end user. This development and support can include vulnerability research and exploit development, malware payload development,

44 As argued in previous work published by the Atlantic Council, proliferation "presents an expanding set of risks to states and challenges commitments to protect openness, security, and stability in cyberspace. The profusion of commercial OCC vendors, left unregulated and ill-observed, poses national security and human rights risks. For states that have strong OCC programs, proliferation of spyware to state adversaries or certain non-state actors can be a threat to immediate security interests, long-term intelligence advantage, and the feasibility of mounting an effective defense on behalf of less capable private companies and vulnerable populations. The acquisition of OCC by a current or potential adversary makes them more capable" (See: Winnona DeSombre et al, *Countering Cyber Proliferation*).

45 "Stalkerware: What to Know," Federal Trade Commission, May 10, 2021, https://consumer.ftc.gov/articles/stalkerware-what-know.

46 IMSI catchers are also referred to as "Stingrays" after the Harris Corporation's eponymous product line; Amanda Levendowski, "Trademarks as Surveillance Technology," Georgetown University Law Center, 2021, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3455&context=facpub.

47 For more see: Winnona DeSombre et al., *A Primer on the Proliferation of Offensive Cyber Capabilities*, Atlantic Council, March 1, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

technical command and control, operational management, and training and support, but need not include all.[48] Limiting the discussion of spyware vendors to only those offering end-to-end capabilities risks obscuring critical commercial relationships significant to this discussion, as will become clear in the cases below. In this dataset, vendors are considered parent companies, or an entity that has a majority or controlling interest in another entity. The total count of vendors includes branches—local offices in a different jurisdiction from the parent firm—while subsidiaries are broken down below. A branch is considered an extension of the parent company whereas a subsidiary is a separate legal entity and has separate legal implications than the parent company. Given legal jurisdiction is important for the purposes of this research, we have considered branches as part of the vendor count while keeping subsidiaries as a separate category.

Individual: An individual, as referred to in this report, is a person who was directly involved with a vendor or supplier, or an entity associated directly with a vendor or supplier. Individuals can be founders of companies, senior management officials, or investors.

Supplier: A supplier sells a component or service used to develop a spyware product but does not directly develop or operate spyware or comparable services. For example, a supplier might sell a vulnerability or a subscription service of exploits to a vendor who then develops the actual software. Suppliers are a crucial but often overlooked part of this market. Those vendors that cannot develop some part of a spyware service in-house—most often the regular supply of software exploits needed for continued access to major operating systems—look to procure these from a supplier.

Partner: As used in this report, a partner is a company that is connected to a spyware vendor, though the nature of the relationship can take a few different forms. First, a partner can be unrelated to the development of spyware itself but important to other operations of the vendor (e.g., marketing or sales services). Second, a partner could provide complimentary surveillance products like telecommunications intercept devices or means to process data gathered from spyware, such as location data mapping tools. A partner can also be described in public statements as a "partner" but without the terms of the relationship further publicly defined (e.g., Nexa Group's relationship to Cytrox AD).

Investor: An entity (a firm, mutual fund, etc.) or individual that commits capital with the expectation of receiving financial returns.[49] There are many different types of investors, including angel investors, venture capitalists, peer-to-peer lenders, personal investors, and institutional investors.[50] This report does not make a distinction between these types of investors or their specific investment strategies. Indeed, many different types of investment are seen throughout the report through individuals, venture capitalists, and government funds, among others.

Holding Company: A holding company is a type of business entity that owns the outstanding stock of other companies.[51] Its primary purpose is to control and manage one or more companies it owns, rather than to produce goods or services itself. Holding companies can own a variety of assets, including shares of other companies, real estate, patents, trademarks, and more. By holding a controlling interest in other companies, a holding company can influence or direct its policies and management decisions. This structure can provide benefits such as risk management, tax advantages, and simplified control over multiple businesses.[52]

Subsidiary: A subsidiary is a company that is more than fifty percent owned by a parent or holding company.[53] Subsidiaries are separate and legally distinct from their corporate parents or holding companies, which typically is reflected in the independence of their governance, financials, taxes, and liabilities. However, parent companies often have considerable influence over their subsidiaries.[54]

The summary profiles of vendors and suppliers can be found in the Trends section of the report, as well as in Appendix A.

48 DeSombre et al., *A Primer on the Proliferation*.

49 Ali Hussain, "What Does an Investor Do? What Are the Different Types?" *Investopedia,* June 22, 2024, https://www.investopedia.com/terms/i/investor.asp#:~:text=Investopedia%20%2F%20Yurle%20Villegas-,What%20Is%20an%20Investor%3F,expectation%20of%20receiving%20financial%20returns.

50 Ali Hussain, "What Does an Investor Do?"

51 "Understanding Holding Companies," *Nelligan Law,* February 8, 2011, https://nelliganlaw.ca/articles/understanding-holding-companies/.

52 "What is a Holding Company Structure and Why is it So Popular," *National Association of Secretaries of States, https://www.nass.org/sites/default/files/2023-07/issue-paper-CT-Corp-NASS-summer23.pdf*.

53 "Subsidiary," *Britannica, https://www.britannica.com/money/subsidiary*.; U.S. Securities and Exchange Commission, "Financial Disclosures about Acquired and Disposed Businesses," *SEC,* https://www.sec.gov/corpfin/financial-disclosures-acquired-disposed-businesses-guidance.

54 James Chen, "Subsidiary Company: Definition, Examples, Pros & Cons," *Investopedia,* June 25, 2024, https://www.investopedia.com/terms/s/subsidiary.asp#:~:text=How%20Subsidiaries%20Work-,Subsidiaries%20are%20separate%20and%20distinct%20legal%20entities%20from%20their%20parent,it%20is%20incorporated%20and%20operates.

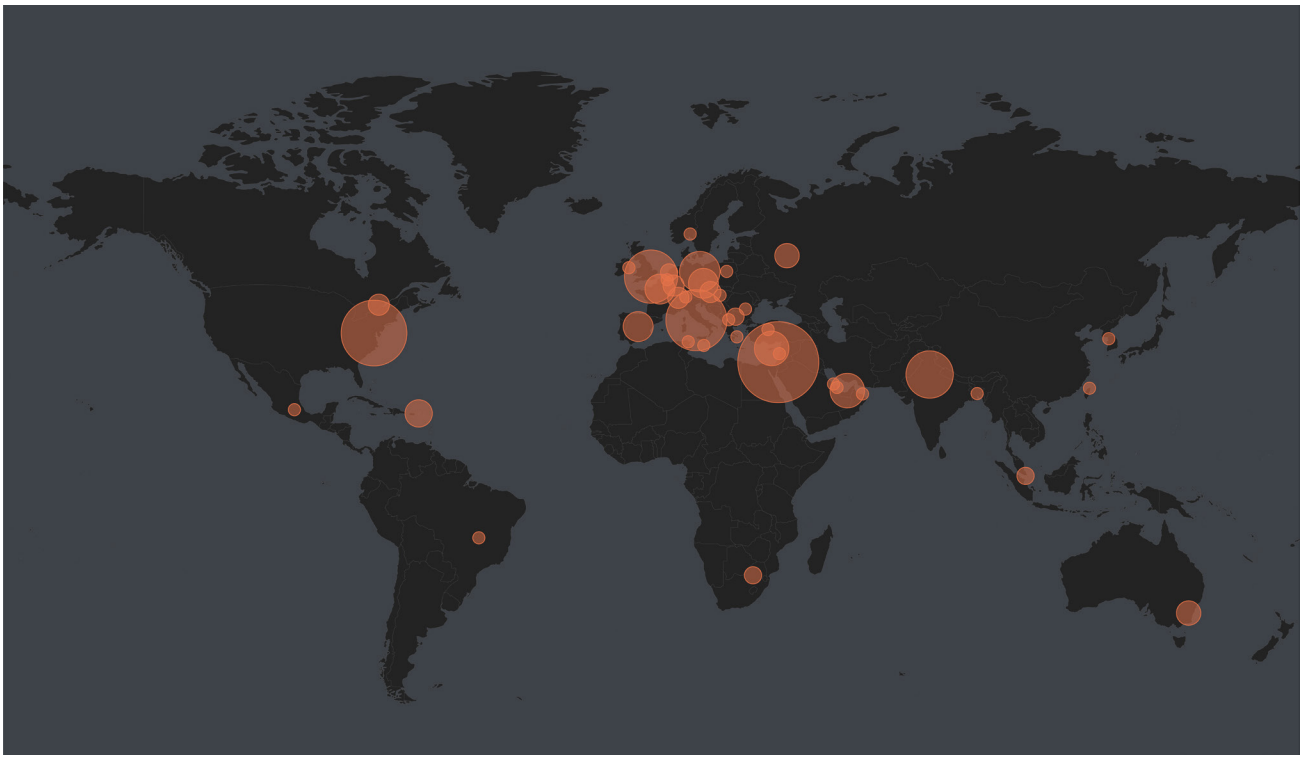

FIGURE 2: Entities in the dataset are spread across jurisdictions

ANALYSIS

This section identifies and explores six distinct trends from the data gathered in this sample of the spyware market:

1. The majority of identified entities in this sample are domiciled in Israel, India, and Italy
2. Serial entrepreneurs are rife
3. The robust partnerships between spyware and hardware surveillance vendors
4. The deliberate and repeated efforts by firms to shift their identities and even corporate structure
5. The movement of those corporate structures across strategic jurisdictional boundaries
6. The significant cross-border mobility of capital supporting spyware development and sales

The dataset is based on a collection of known or reported spyware vendors and analysis, using these as a basis to identify first-order connections and map the resulting network of entities. We included only those entities as defined above. As a result, the dataset is a sample of the spyware market and the trends speak to this data.

1. The Three I's

Across the 435 entities in this sample of the spyware market, there is a significant concentration of vendors and associated entities in three jurisdictions: Israel, India, and Italy. These states are by no means the only hosts of spyware vendors or their investors and partners, but they are unusually prolific.

- **Israeli cluster:** Eight vendors (NSO Group, Saito Tech—formerly Candiru Ltd, Cognyte, Paragon Solutions, MerlinX, Quadream Inc./InReach Technologies Limited, Blue Ocean Technologies, and Interionet.) This cluster comprises 43.9 percent of the entities in this dataset. The average period of activity (from the time of initial registration to the most recent) for each of these vendors is 6.6 years.
- **Indian cluster:** Five vendors (Aglaya Scientific Aerospace Technology Systems Private Limited**,** Appin Security Group, BellTroX Infotech Services Private Ltd., CyberRoot Risk Advisory Private Limited, and Leo Impact Security Service PVT Ltd.) as well as one supplier (RebSec Solutions). This cluster covers 7.8 percent of the entities

in this dataset, with the average period of activity for vendors lasting 10.1 years.

- **Italian cluster:** Six vendors (Dataflow Security s.r.l., DataForense s.r.l., Memento Labs srl—formerly Hacking Team srl or Grey Heron, Movia SPA, Negg Group/Negg International, s.r.l., and RCS ETM Sicurezza S.p.A.) and one supplier (VasTech). This cluster includes 13.6 percent of all entities in the dataset with an average period of activity lasting 6.1 years.

This dataset represents a global market and it is notable that, for all the press on some firms in the country, Israel represents barely half of this sample. It is also important to note that in the early stages of this project, the most widely reported vendors were based in Israel, which means they constituted a much larger portion of early versions of the dataset. Italy is a notable jurisdiction given its home in the EU, where debates continue about how to govern the presence and operation of spyware vendors. The geographic spread of these "Three I's" underscores the need for cooperative approaches to driving transparency and shifting behavior in the spyware markets and highlights the absence of both Israel and India in the most recent high-profile spyware policymaking process, the Pall Mall declaration.[55]

2. Serial Entrepreneurs

Across this sample of the market, there is a recurring pattern of employees, including founders leaving their first firm to found and work in other companies, often repeatedly. This is not unlike other startup cultures where this kind of serial entrepreneurship is common. It is interesting in the context of this market, however, given the essential similarity of these products' intended function and the assumed stickiness of customer relationships with founders and senior employees. Within the dataset, founders of vendors and suppliers are involved in 2.2 companies on average.

Serial Entrepreneurs:

AVERAGE NUMBER OF COMPANIES

2.2%

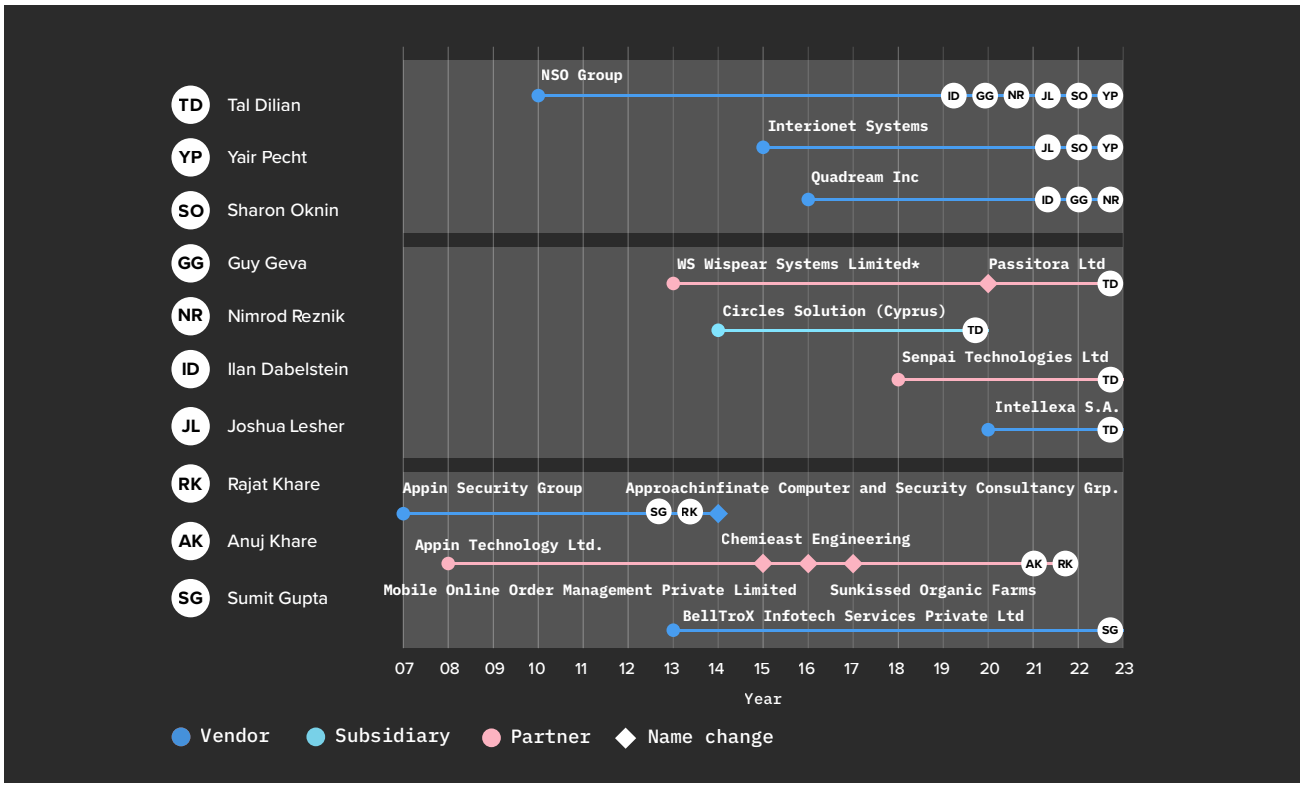

FIGURE 3: Employees frequently make the jump from employee to founder

55 "The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities," February 6, 2024, https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf.

The NSO Group, arguably the most well-known spyware vendor, is a prime example of this phenomenon. The firm was founded in 2010 in Israel by Niv Karmi, Omri Lavie, Shalev Hulio, and Eddy Shalev and is the developer of the Pegasus spyware. Despite investigations from the EU and regulatory action from the US, the firm continues to operate branches in the United States and Luxembourg along with subsidiaries in Bulgaria and Cyprus.[56]

The vendor Quadream Inc., known for the spyware Reign, was founded in 2016 in Israel by former NSO Group employees Guy Geva and Nimrod Reznik, as well as former military official Ilan Dabelstein and goes by the name Kvader Ltd. in Israel.[57] Like Quadream Inc., Interionet Systems Ltd. (Interionet) is an Israeli vendor founded in 2015 by Yair Pecht and Sharon Oknin, former employees of NSO Group.[58] Israeli businessman Joshua Lesher, an NSO shareholder and board member, also sits on Interionet's board.[59]

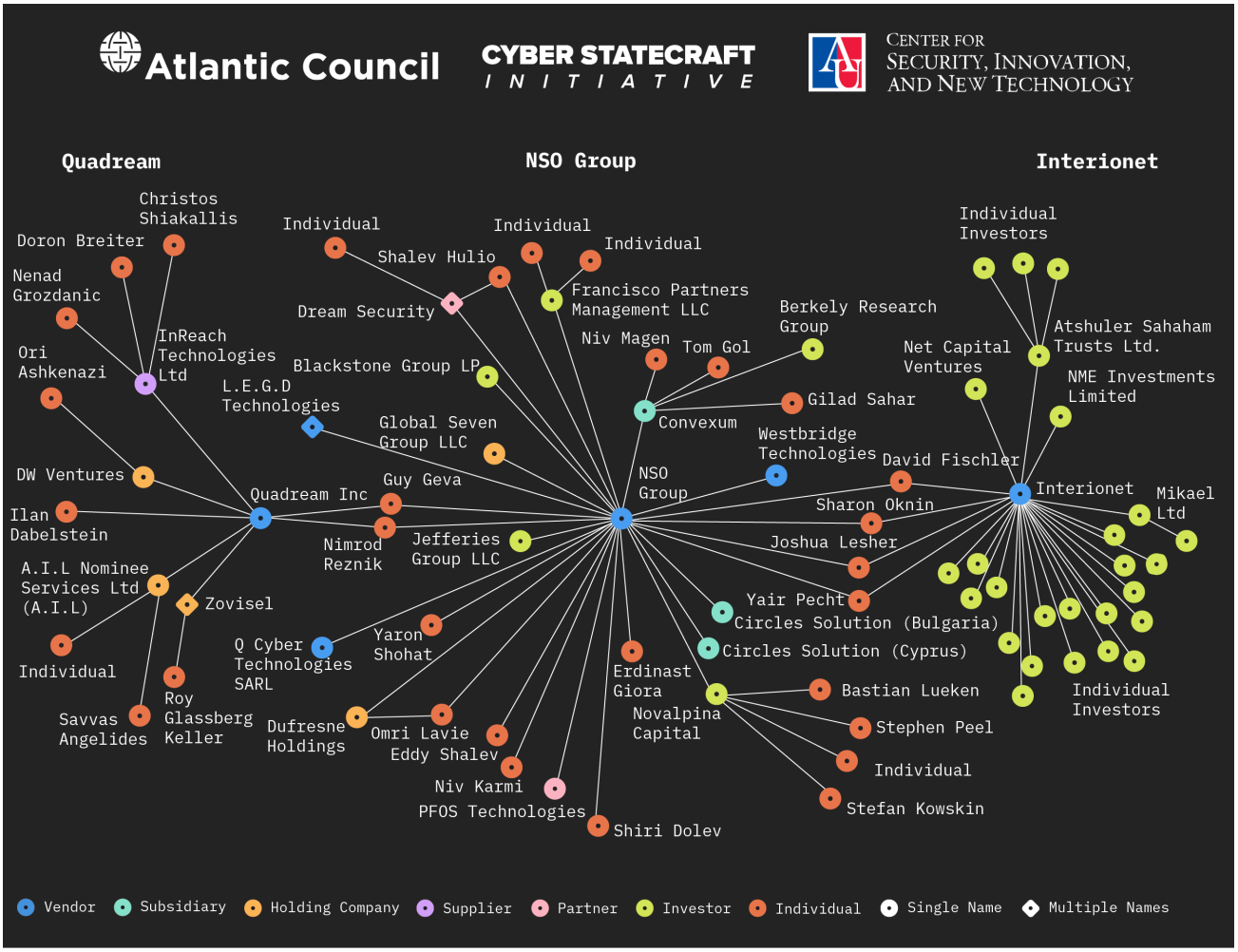

FIGURE 4: Mapping connections in the NSO Group, Quadream, and Interionet clusters

56 "Investigation of the Use of Pegasus and Equivalent Surveillance Spyware," European Parliament, June 2023, https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf; US Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," press release, November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

57 "Online Information and Services — Online Corporations (ONLINE Corporations)," accessed July 3, 2024, https://ica.justice.gov.il/GenericCorporarionInfo/SearchCorporation?unit=8; Bill Marczak et al., *Sweet Quadream: A First Look at Spyware Vendor Quadream's Exploits, Victims, and Customers*, Citizen Lab (Munk School, University of Toronto), April 11, 2023, https://citizenlab.ca/2023/04/spyware-vendor-Quadream -exploits-victims-customers/.

58 "Interionet (Company Profile)," Crunchbase, accessed July 3, 2024, https://www.crunchbase.com/organization/interionet-5cdb; "Interionet (Company Profile)," Datanyze, accessed July 3, 2024, https://www.datanyze.com/companies/interionet/481395181; *NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases*, Citizen Lab (Munk School, University of Toronto), October 29, 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/; Henricks, "All About Holding Companies."

59 "IVC Research Center: Data & Insights," accessed July 10, 2024, https://www.ivc-online.com/.

Interionet "develops malware for internet routers" and is notable for compromising internet-of-things devices, such as video surveillance cameras.[60] In 2022, Interionet won a contract with the Belgian police for their €299 million modernization project called I-Police.[61] In a study of cyber capabilities in the international arms market[62] the authors assessed with high confidence that Interionet "is willing to market its capabilities in countries which are not allied to the American and European interests."[63]

There are examples of this trend outside of Israel as well. Appin Security Group, established by Rajat Khare and his brother Anuj, has since been alleged to have targeted and spied on entities worldwide. Materials online appear to show the company offering hack for hire services.[64] BellTroX Infotech Services Private Ltd. was registered in India in 2013 by Sumit Gupta, formerly an employee of Appin Security Group.[65] BellTrox Infotech Services Private

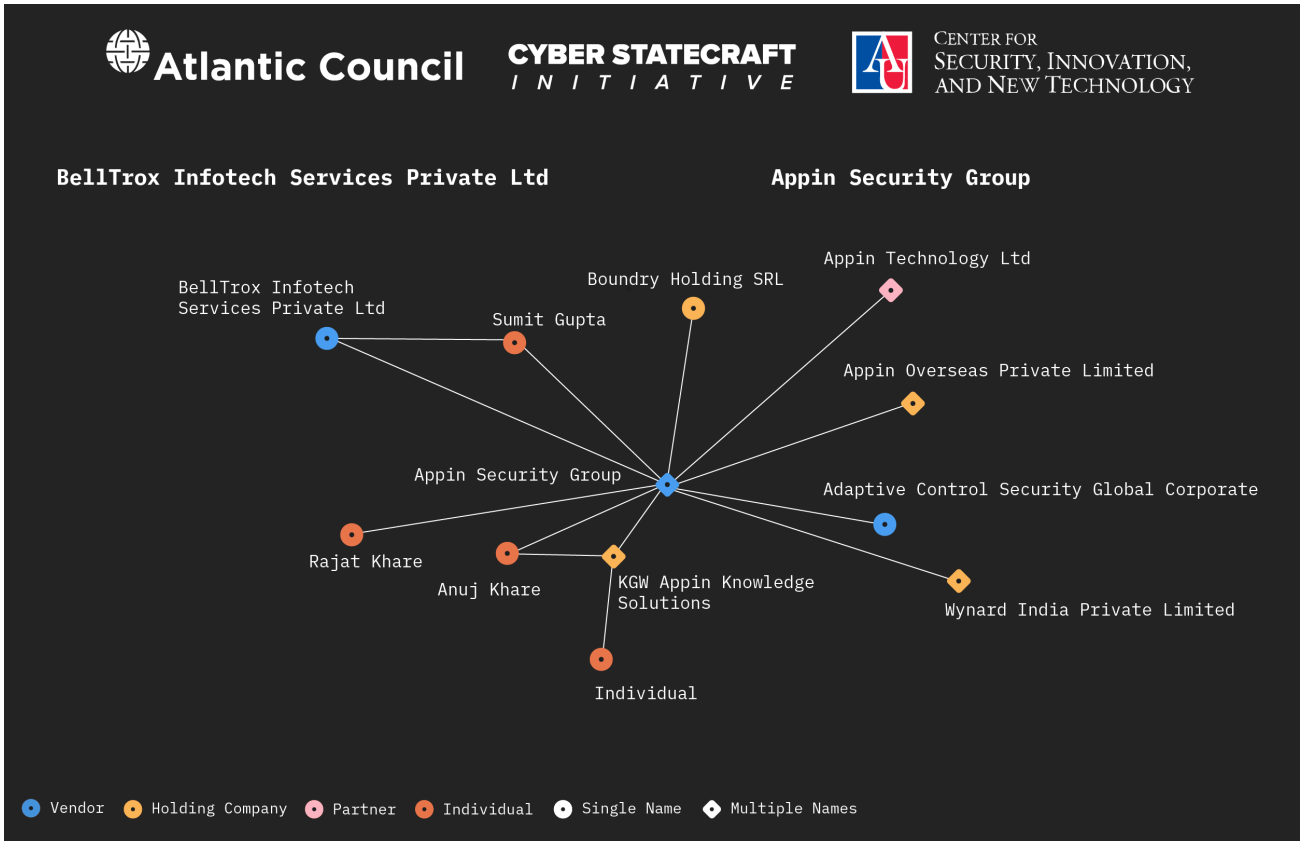

FIGURE 5: Mapping connections in the Appin and BellTrox clusters

60 Becky Peterson, "Inside the Israel Offensive Cybersecurity World Funded by NSO Group," *Business Insider*, September 6, 2019, https://archive.is/MtUPB#selection-2905.1-2905.327; "Interionet," accessed July 10, 2024, https://www.interionet.com/; "Dream Poaches from Tenable, SAT Distributes Kaymera, Fischler at Interionet, Boeing Upheld for DIA Contract," Intelligence Online, March 23, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/03/23/dream-poaches-from-tenable-sat-distributes-kaymera-fischler-at-interionet-boeing-upheld-for-dia-contract,109926917-art.

61 "Interionet Adds Another Israeli Stamp to Belgium's I-Police Programme," Intelligence Online, February 11, 2022, https://www.intelligenceonline.com/surveillance--interception/2022/11/02/interionet-adds-another-israeli-stamp-to-belgium-s-i-police-programme,109840803-art.

62 Winnona DeSombre, Lars Gjesvik, and Johann Ole Willers, *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*, Atlantic Council, November 8, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

63 DeSombre, Gjesvik, and Ole Willers, *Surveillance Technology at the Fair*. Also of note, as recently as in June 2024, Interionet presented its capability to provide access to the information behind dynamic IPs, NAT, and P2P at the ISS World Europe, a trade show for lawful interception and intrusion products (see: "ISS World Training," TeleStrategies, accessed July 10, 2024, https://www.issworldtraining.com/).

64 Appin Documents for Indian Angels Network (ValPro Employee April 4, 2009 Draft Equity Participation Memo)," DocumentCloud, accessed July 10, 2024, https://www.documentcloud.org/documents/23451868-20090506-memo-for-indian-angels-network; Andy Greenberg, "A Startup Allegedly 'Hacked the World.' Then Came the Censorship—and Now the Backlash," *Wired*, February 1, 2024, https://www.wired.com/story/appin-training-centers-lawsuits-censorship/.

65 Raphael Satter and Christopher Bing, "How Mercenary Hackers Sway Litigation Battles," *Reuters*, June 30, 2022, https://www.reuters.com/investigates/special-report/usa-hackers-litigation/.; Appin Security Group had an "infrastructure sharing" relationship with BellTroX Infotech Services Private Ltd, another vendor, in 2013, but it is unclear what the nature of this relationship was and when it ended.

Ltd. has been previously named by Meta as offering "hack for hire" services.[66]

This suggests that more closely governing the talent pools of individuals pivoting between companies might restrict these individuals from creating their own companies and limit the proliferation of spyware vendors. To impede talent from pivoting easily between vendors, export licensing bodies could require more detailed information on key personnel and their past employment to help identify serial offenders of the laws and policies of other jurisdictions. Policymakers should also consider focusing on individuals when attempting to limit harmful activities by a vendor, rather than just the vendor as a business entity, given the fluidity of talent between firms.

3. Partnerships with Hardware Surveillance

Spyware vendors in the dataset have sometimes partnered with hardware-based surveillance companies whose products might complement the functionality of their spyware tools. We have identified nine vendors or suppliers known to have at least one partner, with at least five vendors partnering with at least one hardware company. The most active example of these partnerships is the Intellexa Consortium, encompassing relationships between seven distinct hardware firms.[67] Formed around founder Tal Dilian in 2018, the Intellexa Group comprises several companies including Cytrox AD, WS WiSpear Systems Limited (also founded by Dilian), and Senpai Technologies Ltd.[68] In 2020, Intellexa Group expanded to include Intellexa S.A., formerly known as Intellexa Single Member.[69] Cytrox AD was formed in 2017 by Rotem Farkash and Abraham Rubinstein in North Macedonia and developed the spyware known as Predator. WS WiSpear Systems Limited specializes in intercepting targeted Wi-Fi signals and extracting passwords and communications at long range, and Senpai Technologies Ltd. is an open-source intelligence company that specializes in analyzing data from phones infected with spyware.[70]

> In addition to the Intellexa Group, there is the Intellexa Alliance, formed in 2019 as a partnership between the Intellexa Group and the Nexa Group. Nexa Group is a cluster of four other companies selling interception technology that retail their products together.[71] It remains unclear whether the Intellexa Alliance is still operational, as tensions have emerged between the two entities.[72] Together, the Intellexa Group and Intellexa Alliance comprise the Intellexa Consortium, profiled in more detail in the Cyber Statecraft Initiative's earlier report, "Markets Matter: A Glance into the Spyware Industry."[73]

This trend appears in the Italian market as well, with vendor Memento Labs srl (subsequently known as Hacking Team srl) partnering with South African firm VASTech, founded in 1999 by Frans Dreyer, to develop a passive interception product for wireless communications (building on earlier work from the firm DataVoice).[74] VASTech maintains two offices in South Africa while VASTech AG operates in Switzerland, and VAS Technologies is located in the UAE.[75] VASTech would later go on to propose a

66 Mike Dvilyanski, David Agranovich, and Nathaniel Gleicher, "Threat Report on the Surveillance-for-Hire Industry," Meta, December 16, 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf; In 2020, Citizen Lab connected Dark Basin, a likely state-sponsored actor, to the larger BellTroX Infotech Services Private Ltd's network - John Scott-Railton et al., *Dark Basin: Uncovering a Massive Hack-For-Hire Operation*, Citizen Lab (Munk School, University of Toronto), June 9, 2020, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; Ottavio Marzocchi and Emily (Ai Hua) Gobet, "Briefing for the PEGA Mission to Cyprus and Greece," European Parliament: Policy Department for Citizens' Rights and Constitutional Affairs, November 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/738330/IPOL_STU(2022)738330_EN.pdf.

67 "Intellexa Consortium" is a term the companies have used to market themselves and is the label of choice for the US Department of Treasury's Office of Foreign Assets Control (OFAC) – "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," *U.S. Department of the Treasury,* March 5, 2024, https://home.treasury.gov/news/press-releases/jy2155.

68 Marzocchi and Gobet, "Briefing for the PEGA Mission."

69 "Predator Files: Technical Deep-Dive into Intellexa Alliance's Surveillance Products," Amnesty International, October 6, 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

70 Marzocchi and Gobet, "Briefing for the PEGA Mission"; "Predator Files: Technical Deep-Dive into Intellexa"; Meir Orbach, "The Cyber Company, the Former Officer, and the Lost Money," CTech by Calcalist, October 17, 2019, https://www.calcalistech.com/ctech/articles/0,7340,L-3772040,00.html.

71 Nexa Group comprises Nexa Technologies (now RB 42), Nexa Technologies CZ s.r.o., Advanced Middle East Systems FZ LLC, and Trovicor FZ (alt. Trovicor Intelligence) - "The Predator Files: Caught in the Net" (Amnesty International, October 9, 2023), https://www.amnesty-international.be/sites/default/files/2023-10/act1072452023english.pdf.

72 "The Predator Files: Caught in the Net."

73 Roberts et al., "Markets Matter: A Glance into the Spyware Industry."

74 Roberts et al., "Markets Matter: A Glance into the Spyware Industry"; "VasTech Profile: Version 1," VasTech, February 10, 2008, https://respubca.home.xs4all.nl/pdf/J-LA-001-VT-01-LA-VASTech-profile-2.pdf. Notably, before its demise, the Gaddafi regime heavily relied on Zebra to surveil the entire Libyan population (See: Jenna McLaughlin, "South African Spy Company Used by Gadaffi Touts Its NSA-Like Capabilities," The Intercept, October 31, 2016, https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/).

75 "VasTech Profile: Version 1"; "VASTech AG (Company Profile)," OpenCorporates, accessed July 3, 2024, https://opencorporates.com/companies/ch/1129537.

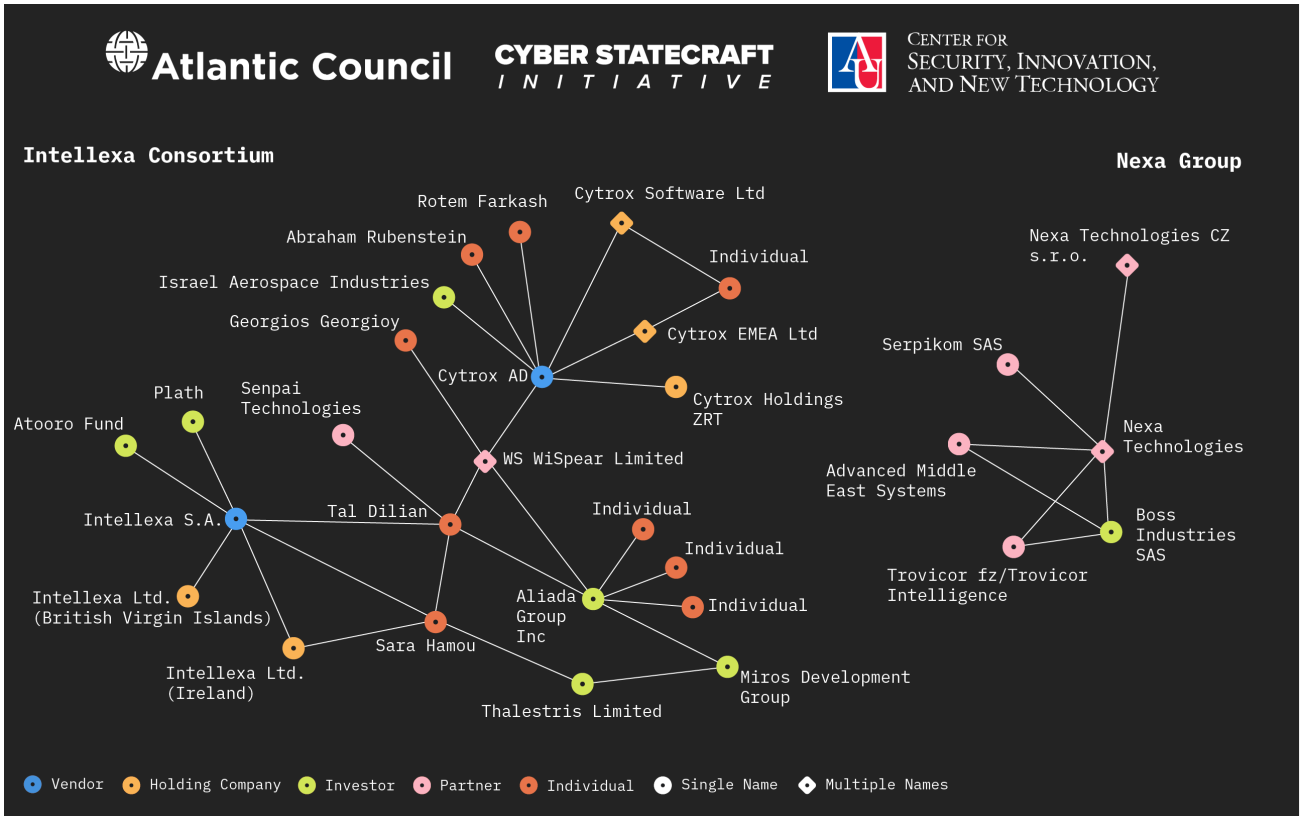

FIGURE 6: Mapping connections in the Intellexa Consortium and Nexa Group clusters

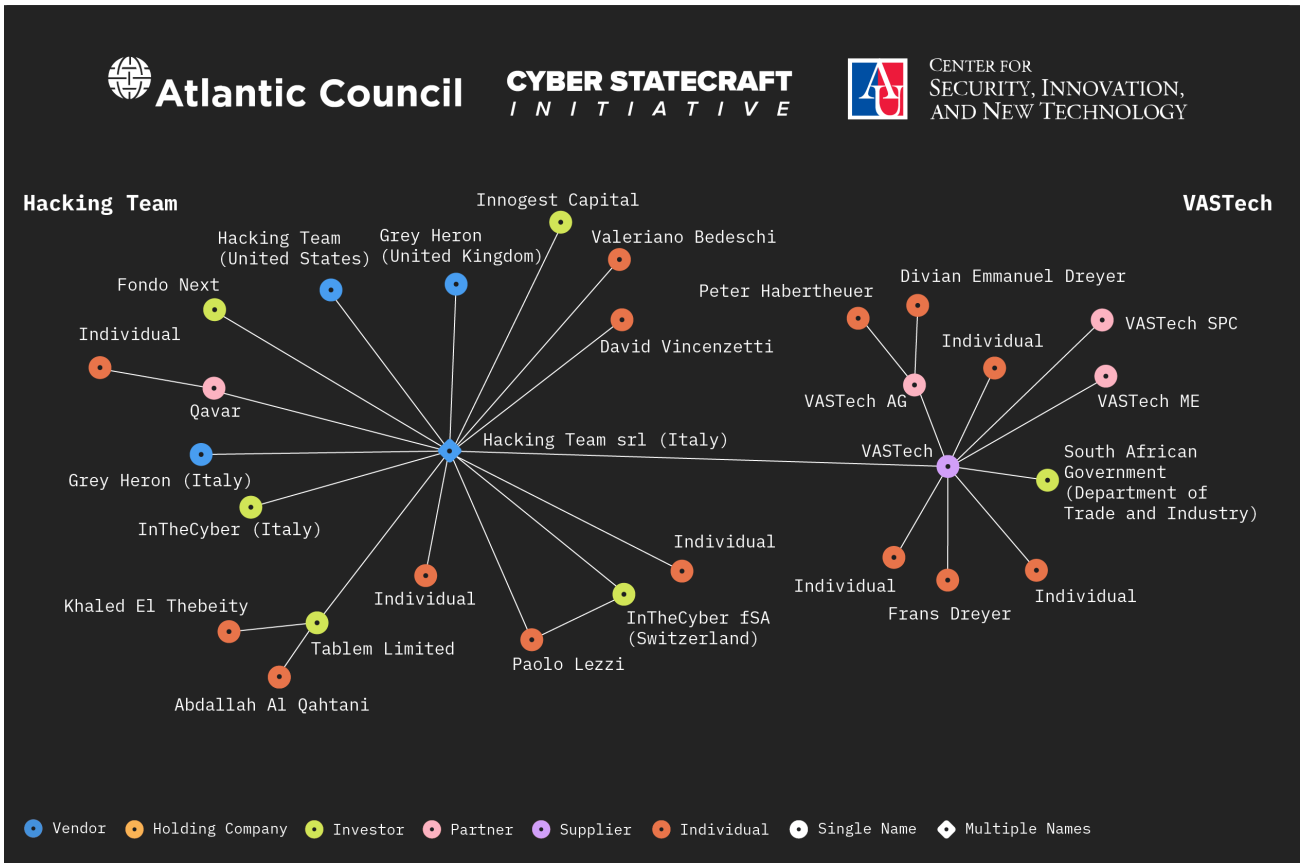

FIGURE 7: Mapping connection between Hacking Team srl and VASTech clusters

partnership with Hacking Team srl to directly resell the vendor's spyware in 2015.[76]

Firms fostering relationships with others offering complementary products is not novel but it is nonetheless interesting to see in this sample of the spyware market. The phenomenon underlines the further importance of policies that address the market as a whole and collaboration across multiple states, as vendor or jurisdiction-specific actions often have limited effect on these wider relationships. Regulating the kinds of support provided to spyware vendors selling to government agencies could help govern the kinds, and content of these partnerships and extend important transparency measures like "Know Your Vendor" requirements to important firms a step beyond the initial spyware transaction. This recommendation is particularly important due to shifting vendor identities.

This trend also highlights the potentially complex relationship between the spyware market and vendors of other electronic surveillance technologies. An open question for further research is how efforts to constrain spyware sales may impact these complementary tools.[77] A further question raised is how substitutable these non-spyware alternatives might be for existing customers and the extent to which spyware firms (like VASTech) offer both spyware and other products to diversify and strengthen their business.

4. Shifting Vendor Identities

Spyware vendors will change legal names and even shift entire corporate structures, which can serve to obscure their identity and, potentially, manage the impact of negative reporting.

Despite name changes, reporting often refers to entities by their most popularized name. This can obscure the vendor's ongoing activity and impede researchers, policymakers, and any firms attempting to exercise due diligence in potential investments. On average, the entities tracked in the dataset changed names more than once, an average of 1.4 times over the time observed, with a name lasting an average of 4.5 years vs. an average vendor lifespan of nearly double that length.

To put this into perspective across the rest of the dataset, 14.3 percent of the vendors underwent a name change while 10.2 percent of all entities changed their name (excluding individuals). Holding Companies had the highest percentage of name changes at 34.4 percent, followed by Vendors (14.3 percent), Partners (20.8 percent), Suppliers (five percent), and Investors (2.1 percent).[78]

The most persistently shifting identity is that of the firm originally known as Candiru Ltd, which changed its name four times over the ensuing nine years, and is known at the time of this writing as Saito Tech Ltd.[79] The vendor originally known as Candiru Ltd was incorporated in 2014 in Israel by founders Ya'acov Weitzman and Eran Shorer.[80] Candiru Ltd has sold products to Hungary, Spain, and the United Arab Emirates, who all used the spyware for political suppression of opposition and civil society.[81] The group's annual name changes between 2016 and 2020 did not come with changes to the corporate structure. In 2021, Candiru Ltd and its associated names were added to the US Entity List alongside NSO Group.[82] In popular discourse, the vendor is often called Candiru Ltd, this report refers to all vendors by their present legal name, which for Candiru Ltd is Saito Tech Ltd.

On the other hand, Memento Labs srl, initially named Hacking Team srl, retained its original brand for sixteen years, the longest of any entity in the dataset, until changing it in 2019. Formed in 2003 in Italy by David Vincenzetti and Valeriano Bedeschi, Hacking Team srl developed the Remote Control Systems (RCS) spyware. A wide breadth of information is available on the business model of Hacking Team srl due to a leak of its internal data in 2015.[83] Hacking Team srl has been reported to sell to Ecuador, Nigeria, and Saudi Arabia, as well as many states, all of which may

76 "Re: (Vastech) Possible visit to Milano," WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024, https://wikileaks.org/hackingteam/emails/emailid/1064489; "R: further conversation," WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024. https://wikileaks.org/hackingteam/emails/emailid/12014; "Re: (Vastech) Meeting" WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024, https://wikileaks.org/hackingteam/emails/emailid/1150073.

77 Hat tip to James Shires for this trenchant point.

78 Percentages are based on excluding individuals from the count and there are no name changes recorded for subsidiaries.

79 Candiru > DF Associates > Grindavik Solutions Ltd. > Taveta Ltd. > Saito Tech Ltd. (2014-2023); "Saito Tech, Formerly Candiru (Company Profile)," Business & Human Rights Resource Centre, accessed July 10, 2024, https://www.business-humanrights.org/en/companies/candiru/?companies=915955.

80 Bill Marczak et al., *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*, Citizen Lab (Munk School, University of Toronto), July 15, 2021, https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/; John Scott-Railton et al., *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*, Citizen Lab, (Munk School, University of Toronto), April 18, 2022, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

81 Feldstein and Kot, "Why Does the Global Spyware Industry Continue to Thrive?"

82 US Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List."

83 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/.

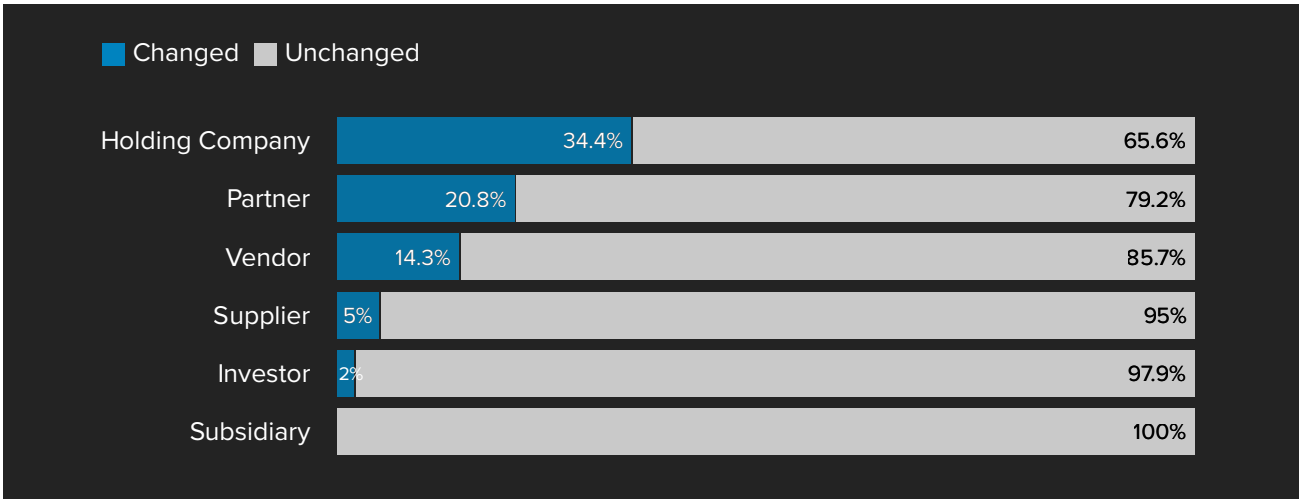

FIGURE 8: Entities change their legal name to obscure their identity and manage the impact of negative press
Note: Data excludes individuals

have utilized the RCS spyware to suppress human rights.[84] Despite legal obstacles, including the revocation of the firm's export license in 2016, Hacking Team srl continued to exist as a company. From 2017 to 2018, there was also a potential spin-off of Hacking Team srl known as Grey Heron, as announced by a Hacking Team srl representative at a security conference in the United Kingdom.[85] The company was officially renamed Memento Labs srl in 2019 after being acquired by InTheCyber Group fSA, a Switzerland-based investor, in an effort to rebrand itself.[86]

Another example of this behavior can be observed in the Indian vendor Appin Security Group. Beginning in 2014, Appin Technology Ltd., Appin Security Group's parent company, began a rapid succession of name changes evolving from Appin Technology Ltd. to Mobile Online Order Management Private Limited, then from this name to Chemieast Engineering, and then from Chemieast Engineering to Sunkissed Organic Farms. Appin Security Group itself also changed names to Approachinfinate Computer and Security Consultancy Grp and then to Adaptive Control Security Global Corporate.[87] This approach echoes Saito Tech's approach of rapid name changes without significant alterations to business structures.

Equus Technologies provides a good example of name changes in response to press and reporting. Founded in 2014 by Matan Markovics, Daniel Hanga, and Tal Tchwella in Israel, Google attributed the firm as the developer of the Lipizzan software in 2017 and labeled the vendor a "cyber arms company."[88] After this reporting, Equus Technologies struggled to recover from reputational damage as it started losing customers and shareholders shrank their positions in the company.[89] Equus then changed its name to

84 Lorenzo Franceschi-Bicchierai, "Hacking Team srl's 'Illegal' Latin American Empire," Vice (blog), April 18, 2016, https://www.vice.com/en/article/gv5v8q/hacking-team-illegal-latin-american-empire. Within this leak were details on how vulnerability- and exploit-deprived Memento Labs srl (then Hacking Team srl) compared to other vendors who develop some of these in-house (at least in part) like Gamma Group or NSO Group - Vlad Tsyrklevich, "Hacking Team srl: A Zero-Day Market Case Study," (author blog), September 26, 2015 [update], https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/.

85 Joesph Cox, "Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware," *Vice,* March 7, 2018, https://www.vice.com/en/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team.

86 This also occasioned a renaming of the spyware product to Dante in 2022 (see: Joseph Cox and Lorenzo Franceschi-Bicchierai, "Memento Labs srl, the Reborn Hacking Team srl, Is Struggling," Vice (blog), March 31, 2020, https://www.vice.com/en/article/xgq3qd/memento-labs-the-reborn-hacking-team-is-struggling; Lorenzo Franceschi-Bicchierai, "New Traces of Hacking Team srl Malware Show the Spy Vendor Is Still in Business," Vice (blog), February 29, 2016, https://www.vice.com/en/article/nz7nm7/new-hacking-team-apple-mac-malware-samples; "Hacking Team srl's Global License Revoked by Italian Export Authorities," Privacy International (blog), April 8, 2016, https://privacyinternational.org/blog/1042/hacking-teams-global-license-revoked-italian-export-authorities; "Italy, UAE: Memento Labs srl Tries to Get Back into UAE Market through Local Distributor SAT," Intelligence Online, January 19, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/01/19/memento-labs-tries-to-get-back-into-uae-market-through-local-distributor-sat,109903859-art; Joseph Cox, "Government Malware Company 'Grey Heron' Advertises Signal, Telegram Spyware," Vice (blog), https://www.vice.com/en/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team.

87 "Appin Companies' Name Change Documents," DocumentCloud, accessed July 10, 2024, https://www.documentcloud.org/documents/23581428-appin-companies-name-change-documents.

88 Megan Ruthven, Ken Bodzak, and Neel Mehta, "From Chrysaor to Lipizzan: Blocking a New Targeted Spyware Family," *Android Developers Blog* (blog), July 26, 2017, https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html.

89 "Israel: Bindecy Lays Hands on Struggling Cyber Security Firm Merlinx, " Intelligence Online, February 6, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/06/02/bindecy-lays-hands-on-struggling-cyber-security-firm-merlinx,109670437-art.

MerlinX between 2017 and 2018.[90] Tal Tchwella, one of its three founders, also left the company.[91] MerlinX was later acquired by Bindecy, an Israeli company specializing in vulnerability research, in 2021.[92]

These various examples show why it is difficult for policymakers and researchers alike to keep track of vendors, creating an illusion that a vendor has ceased operations when they are functioning under a different name. This image grows more complicated with subsidiaries and branches as they too may shift names rapidly, furthering an already opaque market.

To counter this trend, policy solutions can emphasize individual and investor relationships. A baseline improvement for spyware procurement would also be mandatory "Know Your Vendor" requirements to disclose first- and second-order supplier relationships. Better and more consistent transparency from corporate registries would also help establish the link between these identities, even across jurisdictions—which the report turns to next.

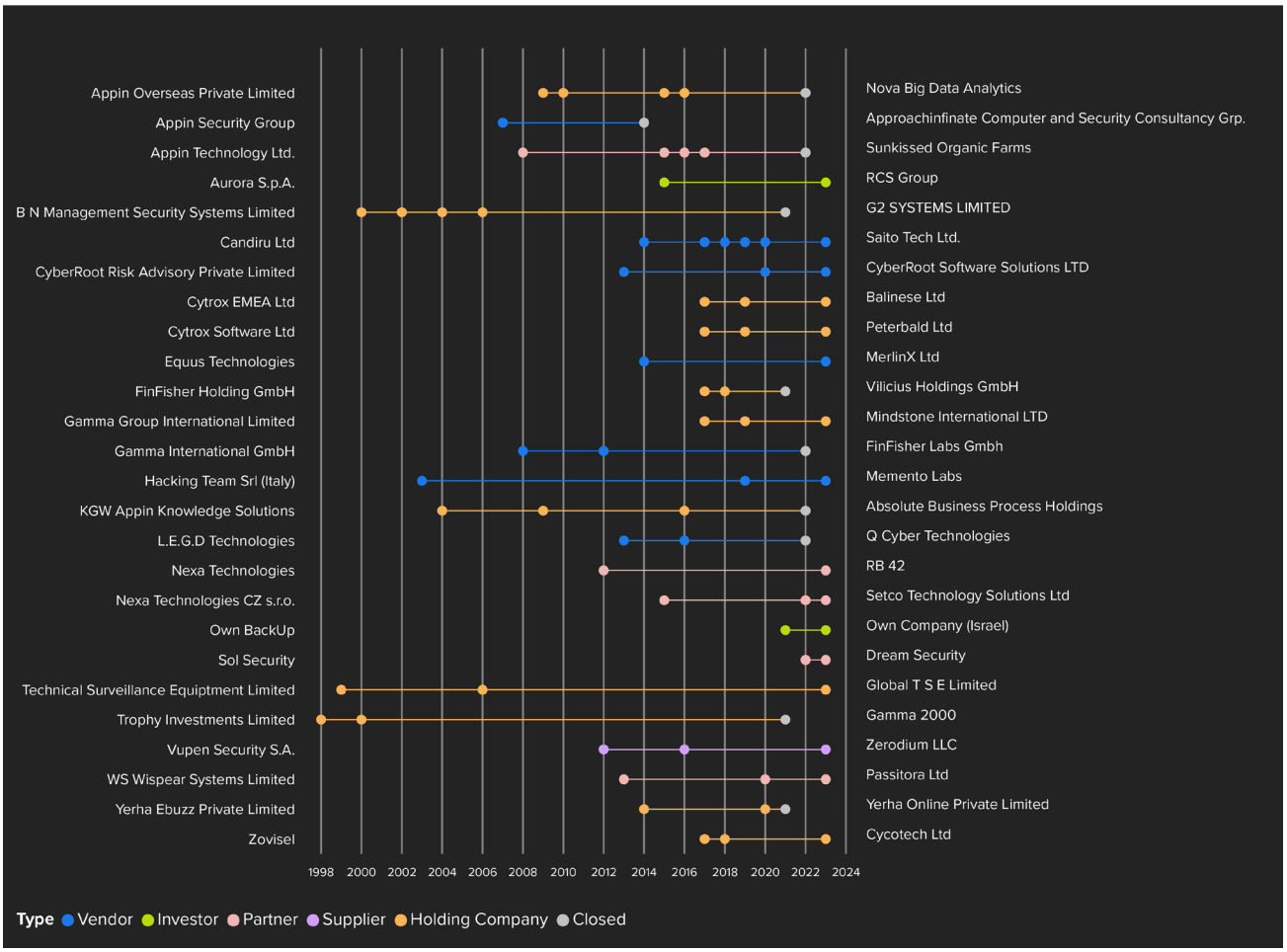

FIGURE 9: Charting entity name changes over time

90 "Israel: Merlinx, Ex-Equus Technologies, Will Bow at ISS," Intelligence Online, February 28, 2018, https://www.intelligenceonline.com/corporate-intelligence/2018/02/28/merlinx-ex-equus-technologies-will-bow-at-iss,108296225-bre.

91 "Israel: Bindecy Lays Hands"; "Israel: Merlinx, Ex-Equus Technologies"; "Tal T. (LinkedIn Profile)," accessed July 10, 2024, https://www.linkedin.com/in/tal-tchwella/; "Israel: Ex-Merlinx Tempt Fresh Start in Cyber with Cyence," Intelligence Online, September 7, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/09/07/ex-merlinx-tempt-fresh-start-in-cyber-with-cyence,109689543-art. ; "Tal T. | LinkedIn." Intelligence Online points to Tchwella leaving "shortly after the Google report" but no source times the departure relative to the firm's name change.

92 "Israel: Bindecy Lays Hands."; According to one corporate registry, MerlinX became inactive in 2022 however, the authors also located annual reports filed by the company with the Israeli Corporations Authority of the Department of Justice that mention its corporate status as "Active" as recent as 2024 - "Merlinx," accessed July 3, 2024, https://finder.startupnationcentral.org/company_page/equus-technologies.; "Online Information and Services - Online Corporations (ONLINE Corporations)," accessed July 3, 2024, https://ica.justice.gov.il/GenericCorporarionInfo/SearchCorporation?unit=8.

5. Strategic Jurisdiction Hopping

Several of the vendors captured in the dataset appear to have constructed subsidiary, branch, and partner relationships that cross strategic jurisdictional boundaries. These relocations may offer a variety of location-specific benefits, from facilitating sales to the EU market with an EU-domiciled firm to situating branches in states with more forgiving laws.

In 2017, the Israeli vendor Quadream Inc. set up a supplier, InReach Technologies Limited, in Cyprus which Quadream Inc. claimed in a later court filing was for the "sole purpose of promoting Quadream Inc. products within the European Union."[93] InReach Technologies Limited's financial structure also included A.I.L Nominal Services Ltd. (A.I.L), similarly established in Cyprus in 2010 as a holding company, with an individual with a relationship to the Ministry of Defense.

Quadream Inc. and InReach Technologies Limited's relationship deteriorated in 2020 and they became entangled in a court case against one another.[94] While the relationship was strained, it is unclear whether the companies formally separated by the time Citizen Lab released Quadream Inc.'s toolkit in 2023, exposing the company's capabilities. This led to the company reporting that it would be shutting down operations although the company is still registered in Israel.[95]

The Intellexa Consortium provides another example of this jurisdictional hopping. One investigation discovered through leaked documents shows how the organizer of the Intellexa Consortium, Tal Dilian, and his partner Sara Hamou, utilized Cyprus as a hub for the Predator spyware to gain access to the European market.[96]

Memento Labs srl (formally known as Hacking Team srl) provides an interesting exception to this trend as its founders appear to have worked to make it strictly an Italian-based vendor. Like models found in other businesses that boast national pride, Hacking Team srl is proud to be "Made in Italy."[97] Their investor base is also mainly Italian, with only two other European countries (Cyprus and Switzerland) present.[98]

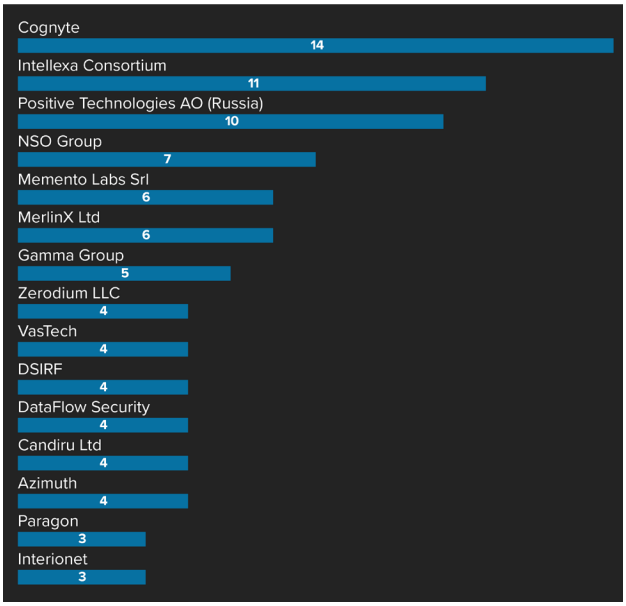

FIGURE 10: Vendors across the dataset can be found in anywhere from one to fourteen jurisdictions
Note: Chart includes entities with three or more jurisdiction locations

National laws governing the behavior of subject firms are largely premised on the common recognition by both the regulators and the regulated of sovereign boundaries. These boundaries delimit the application of law between, say, France and the United Kingdom. The deliberate construction of branch and subsidiary relationships to cross these boundaries may offer firms a measure of protection from regulatory approaches like export controls and create significant opacity in their operations and supply chains by wrapping even loose cross-border relationships in the cloak of "internal" corporate activity. The pivot of vendors to less restrictive jurisdictions reduces the efficacy of export controls and policy action must better limit the effects of jurisdictional arbitrage. But this trend is not limited to corporate organization, indeed it is reflected in capital flows as well, leading to the final trend.

93 Sourced from "court documents obtained from the District Court of Limassol in Cyprus" per Marczak et al., *Sweet Quadream a*nd the original InDream Cypriot registration (see: "InReach Technologies Limited Technologies Limited," CyprusRegistry, accessed July 3, 2024, https://cyprusregistry.com/companies/HE/373827).

94 Marczak et al., *Sweet Quadream.*

95 Ravie Lakshmanan, "Israeli Spyware Vendor Quadream to Shut Down Following Citizen Lab and Microsoft Expose," *The Hacker News*, April 17, 2023, https://thehackernews.com/2023/04/israeli-spyware-vendor-quadream-to-shut.html.

96 David Kenner and Eve Sampson, "Spyware firm Intellexa hit with US Sanctions after Cyber Confidential Exposé, *International Consortium of Investigative Journalists,* March 6, 2024, https://www.icij.org/investigations/cyprus-confidential/spyware-firm-intellexa-hit-with-us-sanctions-after-cyprus-confidential-expose/.

97 Cox and Franceschi-Bicchierai, "Memento Labs srl, the Reborn Hacking Team srl"; Howell O'Neill, "The Fall and Rise of a Spyware Empire." One non-public source suggested Memento Labs srl might have recently renamed itself to "M-Labs".

98 There is comparatively little open-source reporting on Grey Heron.

FIGURE 11: Entities in the dataset cross jurisdictional boundaries

6. Money From Across the World Fuels the Spyware Market

Investors in spyware vendors often cross borders with their capital. Like more conventional markets, spyware vendors and suppliers feature an investor base domiciled in many different jurisdictions. Investment in spyware vendors and suppliers is understudied, despite being a factor in the proliferation of this technology. The sample of the spyware market captured by this dataset includes ninety-five investors identified to date. Among these, outside of investors for whom location was not listed, four jurisdictions were most frequently represented: Italy, Israel, the United States, and the United Kingdom—comprising 46.3 percent of all investors.

The character of spyware investment varies from venture capital, private equity, and government loans to outright acquisitions and direct equity ownership. On average in this dataset, each vendor and supplier had 4.75 identified investors, with Figure 12 highlighting where investors are domiciled and to which cluster they invest. For example, the dataset documents fourteen different US entities investing in spyware vendors or suppliers, the bulk of whom (in twelve of the fourteen cases) are based in Israel. Of note, the Israeli and Italian investors captured in this dataset were likely to mostly invest in their own markets versus the United States and the United Kingdom, whose investors largely sent their capital abroad.

A specific example of this trend is Paragon Solutions. Paragon was established in 2019 in Israel by Ehud Schneorson, Idan Nurick, Igor Bogudlov, and Liad Avraham.[99] A few years later in 2022, the firm established Paragon Solutions US, a US-domiciled subsidiary.[100] Since its establishment, Paragon has made deliberate efforts to break into the US market. Paragon Solutions also has two US-based investors. Battery Ventures, considered to be one of the world's top venture capital firms and headquartered in Boston, is an investor in Paragon Solutions as of this writing.[101] It is also supported by Blumberg Capital, another large US venture capital firm.[102]

Saito Tech Ltd and NSO Group also have investors domiciled in foreign jurisdictions. Saito Tech Ltd had the

99 Thomas Brewster, "Meet Paragon: An American-Funded, Super-Secretive Israeli Surveillance Startup That 'Hacks WhatsApp And Signal,'" *Forbes*, July 29, 2021, https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/.

100 "Israel, United States: Israeli Cyber Firm Paragon Beefs up US Subsidiary," Intelligence Online, August 31, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/08/31/israeli-cyber-firm-paragon-beefs-up-us-subsidiary,110037838-art.

101 "List of all companies," Battery Ventures, accessed July 11, 2024, https://www.battery.com/list-of-all-companies/. The listing does not name "Paragon Solutions US".

102 "Blumberg Capital Alumni Founded Companies," *Crunchbase,* Accessed July 27, 2024, https://www.crunchbase.com/hub/blumberg-capital-alumni-founded-companies.

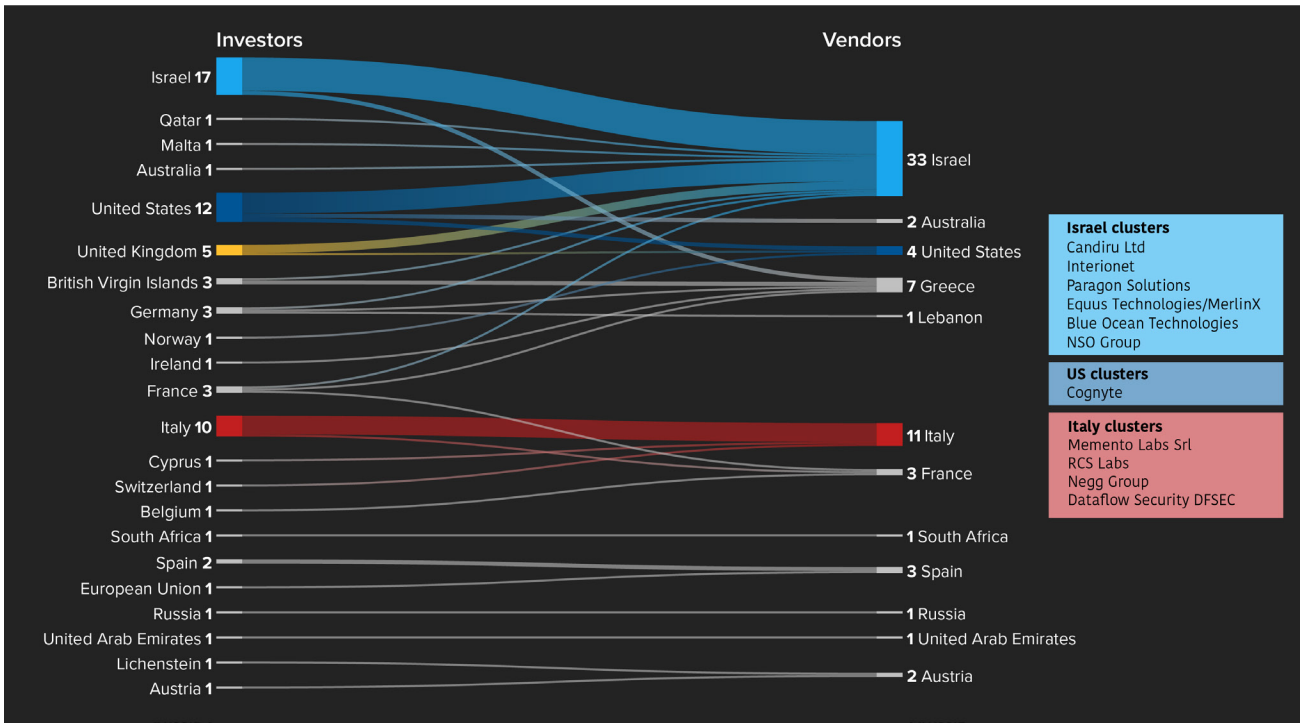

FIGURE 12: Money flows from investors to vendors, often crossing borders. Almost 50% of investors are incorporated in **Israel**, the **United States**, **Italy**, and the **United Kingdom**
Note: Countries are sorted to reduce overlaps.

US-based Founders Group and NSO Group's current and past investors include those domiciled in the United Kingdom, like Novalpina Capital, and in the United States, like Francisco Partners Management, Berkely Research Group, and Blackstone Group LP.[103] The transition in NSO Group investors from Novalpina Capital to other investors took a few years and is well covered in the press.

These cross-border capital flows highlight the importance of international cooperation, and perhaps the central role of the United States and EU, in applying more granular controls and scrutiny on investor relationships in the spyware market.

Improving corporate transparency requirements, such as the US's recent move to compel companies to report their beneficial owners in line with policies in other countries, will support improved investor due diligence and deal review inside the United States.[104] For vendors located outside the US, a recent notice of proposed rulemaking to extend US security review over some forms of outbound investment could provide the basis to catalog and potentially block investment.[105] Targeted sanctions are another option for limiting investors' behavior via designating spyware vendors, blocking financial transactions, or designating investors themselves if their actions fall under the scope of spyware-related sanctions authorities. The use of unilateral sanctions is an active and much-debated topic in both the cybersecurity sector and the wider national security policymaking landscape and this report offers a more fully articulated set of policy recommendations based on these trends and the totality of this dataset in the next section.

103 Thomas Brewster, "Meet Candiru – The Mysterious Mercenaries Hacking Apple And Microsoft PCs For Profit," *Forbes*, October 3, 2019 https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/?sh=4825751d5a39; "Private Equity Owner of Spyware Group NSO Stripped of Control of €1bn Fund," *Financial Times, https://www.ft.com/content/d88518dd-7c66-48b2-b3e5-c765ebe720ab*; "NSO Group's management buys firm from Francisco Partners," *Reuters,* February 14, 2019, https://www.reuters.com/article/idUSL5N209642/; Stephanie Kirchgaessner, "US consultants lined up to run fund that owns Israeli spyware company NSO Group," *The Guardian*, July 31, 2021, https://www.theguardian.com/news/2021/jul/31/nso-group-israeli-spyware-company-berkeley-research-group.

104 "New Rules Require Beneficial Ownership Reporting to FinCEN," Grant Thornton, March 4, 2024, https://www.grantthornton.com/insights/alerts/tax/2024/insights/new-rules-require-beneficial-ownership-reporting-fincen.

105 See the Treasury Department's Notice of Proposed Rulemaking – "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern", US Department of the Treasury, July 5, 2024, https://www.federalregister.gov/documents/2024/07/05/2024-13923/provisions-pertaining-to-us-investments-in-certain-national-security-technologies-and-products-in and the original direction in Executive Order 14105 "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern," August 9, 2023, https://home.treasury.gov/system/files/206/Executive%20Order%2014105%20August%209%2C%202023.pdf.

POLICY RECOMMENDATIONS

The 2024 Report on the Cybersecurity Posture of the United States from the Office of the National Cyber Director (ONCD) lists the growing market of "sophisticated and invasive cyber-surveillance tools" as one of the trends driving change in the United States' cyber strategic environment in 2023.[106] The UK and French governments have made the proliferation and irresponsible use of commercial cyber intrusion capabilities an important and ongoing policy activity, most notably by leading the deliberately multilateral Pall Mall Process on Cyber Intrusion Capabilities.[107] A European Parliamentary committee (the PEGA committee) highlighted the importance of the spyware market as a topic for policymaking and its implications for technology policy, human rights, and national security across the EU's complex network of delegated powers. These efforts are part of a degree of sustained attention on spyware not seen in the previous decade. The authors are encouraged to note the effective adoption of some of their previous recommendations.[108] However, much remains to be done.

The final section of this report presents a set of policy recommendations to further advance these efforts. Not every action identified here is suitable for every state. The United States has outsized authorities and resources and sits in a unique position in the international financial system. Bearing that in mind, however, these recommendations envision a necessary cooperative international approach, conscious of the clear trend of the spyware market's global infrastructure. While a well-regulated and more transparent market will not entirely prevent proliferation, it can be better channeled, subjected to controls, and made less opaque and harmful, as done with other markets of dual-use goods.

FIGURE 13: Mapping spyware trends to policy recommendations

106 Harry Coker, Jr., "2024 Report on the Cybersecurity Posture of the United States," (Washington DC: Office of the National Cyber Director, May 2024), https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf.

107 "The Pall Mall Process: Tackling Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities, UK Foreign, Commonwealth & Development Office, February 6, 2024, https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf.

108 DeSombre et al., *Countering Cyber Proliferation*; The White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse;" "The Pall Mall Process: Tackling Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities."

This project is focused on the spyware market, with the goal of fostering greater transparency across the market, limiting jurisdictional arbitrage, and more effectively scrutinizing supplier and investor relationships. These recommendations are built on a sample of this market, not a final and definitive record of all entities and relationships. Achieving these policy goals would address significant opportunities to limit the risks and harms stemming from the proliferation of spyware. These include more granular and effective policies on vendor behavior, a robust investor due diligence regime, information-rich government risk assessments prior to procurement, and credible legal support for greater long-term transparency in the market.

1. Mandate "Know Your Vendor" requirements

If the defining characteristic of spyware acquisition should, in theory, be an exercise of due diligence, then a marked gap in current policy is the ability to exercise that diligence in the face of shifting vendor identities and supply chains. There is, however, a practical solution: employing "Know Your Vendor" (KYV) requirements. Building on previous recommendations made by the Cyber Statecraft Initiative, the United States and, at a minimum, the sixteen additional signatories to the Joint Statement, should enforce KYV requirements that spyware vendors disclose supplier and investor relationships.[109] This is a credible step toward better information about the segments of the spyware market with which these governments might do business. Such a KYV requirement, implemented consistently across these states, would present a united front to many of the vendors covered in this report who claim to work only with "government" and "Western government" clients. This would also mitigate the potential impact of individual governments fearing vendors would turn down their business.

KYV would create a more consistent reporting environment on the spyware market in these states, providing government clients with the ability to check where their prospective supply chain might include firms on restricted entity lists before awarding contracts. With straightforward information sharing, KYV would also enable long-term efforts to reduce government dollars flowing to high-risk suppliers or vendors. A more effective version of these requirements could mandate disclosure of firms further down the supply chain (suppliers to the suppliers of a vendor).

The United States could set KYV requirements through the US Federal Acquisition Regulatory Council, which would require an update to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) to mandate that any company submitting a bid for a government contract for cyber operations to disclose a list of their vendors and suppliers, investors, and any parent corporate or holding entity. A notice and comment period for such a requirement would likely see vendors request more targeted disclosure requirements for larger conglomerate firms and mechanisms to scope KYV to spyware business units in these firms would be appropriate. KYV would also complement and be strengthened by more effective beneficial ownership requirements.

2. Improve government-run corporate registries

Similar to KYV, government-run corporate registries are a resource for due diligence and accountability. These registries would play a significant role in a more assertive policy regime that addresses the cross-border movement of, or investment in, spyware vendors. These registries would also be an important source of information for due diligence by potential investors as well as provide improved visibility into business entities operating within respective jurisdictions.

For corporate registries to become sources of truth on business and financial structure and histories of vendors, they must be comprehensive, openly accessible to the public, and have verified information. However, currently, the information in corporate registries varies from country to country. For example, the corporate registry of Czechia is comprehensive and contains information about the different names a company has used since its inception, its history of investment by various investors, as well as the individuals who held senior executive offices and their tenures.[110] In contrast, the registries in India and Israel provide only basic information about entities such as the legal name of the corporation, address, date of incorporation, and registration number.[111] In the United States, every state maintains a separate corporate registry of the entities incorporated in their jurisdiction.

109 DeSombre et al., "Countering Cyber Proliferation."; The countries who have signed the Joint Statement are Australia, Canada, Costa Rica, Denmark, France, Finland, Germany, Japan, New Zealand, Norway, Poland, Ireland, Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States. "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware."

110 Transparent Data, "Czech Companies API: Meet Business Register of the Czech Republic." Medium (blog), December 2, 2020. https://medium.com/transparent-data-eng/czech-companies-api-meet-business-register-of-the-czech-republic-78ab563dee92; Transparent Data, "European Business Registers – Comparison of Registry Data on Foreign Companies," Medium (blog), September 10, 2021, https://medium.com/transparent-data-eng/european-business-registers-comparison-of-registry-data-on-foreign-companies-3dda4d32061c.

111 "מינוקמ מיתורשו עדימ - תשרב מידיגאת (מידיגאת ONLINE)." Israeli Corporations Authority accessed July 10, 2024.

2.1 Expand the minimum scope of data captured by registries

National regulations should determine requirements about the categories and corresponding details present in their corporate registries.[112] They should include basic company information (name, registration number, payment ID, address, contact details, and date of registration), ownership details (senior executives, management board, and actual beneficiaries), the number of employees, financial information (balance sheet, cash flow, income statements, and investors), history of name changes, and the legal status of activity (liquidated, active, or bankrupt). This information serves as a bare minimum but could be expanded to include a history of mergers and acquisitions, legal actions against the firm, and active export licenses.

In the United States, this could be accomplished through the National Association of Secretaries of State (NASS) providing guidance to each of the fifty US states. Alternatively, given some risk of a race to the bottom between US states eager to attract corporate activity, the IRS could publish this data where it is collected for Federal purposes.[113]

Outside the US, given the global nature of the spyware market, there is merit in improving corporate registries, especially for the seventeen countries signed on to the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. As the Joint Statement evolves, the Department of State's Bureau of Cyberspace and Digital Policy should consider developing subject-specific working groups—including one on corporate registries and associated information—to bolster harmonization and information sharing across signatories. These countries should seek to work towards seamlessly sharing this registry data where it is not made public. Regularly cross-referencing information on a vendor, especially ones with branches or subsidiaries in multiple countries, can be beneficial in avoiding jurisdictional hopping and arbitrage.

2.2 Expand beneficial ownership identification

In January 2024, the US Department of the Treasury unveiled its Beneficial Ownership Program (BOP), seeking to improve corporate filings on the "persons who ultimately own or control the company."[114] Most countries, however, do not have reporting requirements on beneficial ownership, and many that do have insufficient standards.[115] Better recognition of the beneficial owners behind spyware vendors and, eventually, suppliers, would provide a strong counter to many of the identified trends in this report.

Further improvements can be made to BOPs worldwide. Analysis of beneficial ownership registries of G7 countries Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States (all of whom, except for Italy, are signatories of the Joint Statement) showed that while these countries maintain beneficial ownership registries that require companies to report individuals who own twenty-five percent or more of the shares and voting rights or exert significant control over the management of the company, most do not require any identification document to be submitted by such individuals for verification.[116]

While the US entity that is responsible for beneficial ownership registration, the Department of Treasury's Financial Crimes Enforcement Network (FINCEN), requires entities to provide an image of an identification document for every beneficial owner, the United Kingdom's Companies House register takes no steps to verify name or address data provided by applicants.[117] As highlighted by the capital crosses borders trend, the United States and the United Kingdom are two (of several) concentrated hosts of investors in the spyware market in the sample provided by this dataset. It is especially important for these jurisdictions to improve their methods for identifying beneficial owners.

Other signatories of the Joint Statement do not have BOPs. Transparency Data's study of European business registers reveals that out of the eleven central and eastern European countries that they analyzed, only three required companies to provide information about actual beneficiary owners. Finland, Sweden, and Switzerland (all signatories on the Joint Statement) do not even require information about the founders or owners of companies.[118]

Beneficial ownership transparency is endorsed and monitored by several international organizations, such as the Financial Action Task Force (FATF) and the OECD's Global Forum on Transparency and Exchange of Information for

112 "Initiatives," National Association of Secretaries of State (NASS), accessed July 11, 2024, https://www.nass.org/initiatives.

113 Hat tip to Winnona DeSombre for this clear-eyed view of corporate registration.

114 Financial Crimes Enforcement Network, "FinCEN Issues Final Rule for Beneficial Ownership Reporting to Support Law Enforcement Efforts, Counter Illicit Finance, and Increase Transparency," press release, US Department of the Treasury, September 29, 2022, https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-beneficial-ownership-reporting-support-law-enforcement.

115 "Open Ownership Map: Worldwide Action on Beneficial Ownership Transparency," Open Ownership, n.d., accessed July 10, 2024, https://www.openownership.org/en/map/.

116 "Snapshot of Beneficial Ownership Registries in G7 Countries," Athennian, n.d., accessed July 10, 2024, https://www.athennian.com/post/snapshot-of-beneficial-ownership-registries-in-g7-countries.

117 "Companies House: What Is It and How Is It Failing to Do It," Bureau of Investigative Journalism, n.d., accessed July 10, 2024, https://www.thebureauinvestigates.com/explainers/companies-house-what-is-it-and-how-is-it-failing-to-do-its-job/.

118 Transparent Data, "European Business Registers – Comparison of Registry Data. on Foreign Companies."

Tax Purposes.[119] The seventeen countries that are signatories of the Joint Statement without BOP programs or reporting requirements on founders or owners of companies should enact reporting requirements within their respective jurisdictions which harmonize with both US approaches and global best practices.

2.3 Make government-run corporate registry data public

A final improvement to these registries would be to provide universal public access to their data, in all jurisdictions. OpenCorporates' report, "The Closed World of Company Data," scores countries on the openness, depth, and accessibility of national corporate data records.[120] While the average score is only twenty-two percent of the maximum, several major states—Spain, Greece, and Brazil—scored 0, which means that their corporate registers cannot even be searched without some form of payment.[121] The United Kingdom's scored highest while the United States was only a few ticks above the average.[122] The poor quality of these records hampers due diligence efforts by many actors. For example, high-quality and publicly accessible corporate databases would provide raw informational material for a significantly enhanced investor due diligence regime in the spyware market. It would also help to level the playing field between regulators in different jurisdictions. This would enable cross-border collaboration in regulating the behavior of spyware vendors, suppliers, and investors. This would also allow entities subject to customer due diligence (e.g. banks, notaries, corporate service providers) to improve their verification processes and report discrepancies.

3. Enrich, audit, and publish export licenses

Export licensing requirements are a mechanism for governments to limit the sale and use of certain products and services outside of their borders. Export licenses are a complex domain characterized by significant inter-state variability in standards, covered goods, and application of broader tests of public interest, such as human rights considerations.[123] Indeed, authorities may deprioritize human rights risks if countervailing considerations such as industry growth or perceived geopolitical influence weigh in favor of license approval.[124] The Joint Statement commits its signatories to implement export controls on spyware technology in accordance with their respective laws and regulations.

Certain spyware vendors, like NSO Group, have publicly capitalized on the fact that their exports are licensed by government agencies as an indication of their lawfulness.[125] Decoupling licensing decisions made in deliberate furtherance of geopolitical goals over those dominated by commercial considerations is a tricky and ongoing research question.[126] As noted by the UN Special Rapporteur on Freedom of Opinion and Expression, the global export control framework and its national implementation in areas where NSO Group operates are inadequate for regulating surveillance technology or accounting for human rights impacts.[127] The result is that while NSO Group's exports are indeed "licensed," these and those of other vendors could still present a grave risk to human rights, especially in jurisdictions where the legal framework governing the use of its product is minimal or even nonexistent.

119 "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations," Financial Action Task Force, (Paris, France), November 2023 [update], https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf; "Global Forum on Transparency and Exchange of Information for Tax Purposes," n.d., United Nations, https://www.un.org/esa/ffd/wp-content/uploads/sites/3/2017/05/Global-Forum_-info-sheet-2017.pdf.

120 "The Closed World of Company Data: An Examination of How Open Company Data Is in Open Government Partnership Countries," OpenCorporates, August 4, 2012, https://web.archive.org/web/20120804043101/http://opencorporates.com/downloads/ogp_company_data_report.pdf; "Members of Open Government Partnership," Open Government Partnership, n.d., accessed July 10, 2024. https://www.opengovpartnership.org/our-members/; "OGP Open Company Data Survey Results – Google Sheets," n.d., accessed July 10, 2024, https://docs.google.com/spreadsheets/d/1J0f-lnGNz3qzMDNjacOmLtPiIVPhEZmp_itrfhVGcv8/edit?gid=0#gid=0.

121 Countculture, "How Open Is Company Data in Open Government Partnership Countries?" OpenCorporates (blog), April 16, 2012, https://blog.opencorporates.com/2012/04/16/how-open-is-company-data-in-open-government-partnership-countries/.

122 "OGP Open Company Data Survey Results – Google Sheets."

123 "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect, and Remedy' Framework," United Nations Human Rights Office of the High Commissioner, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.; Curtis Domek and Julien Blanquart, "A New Era of Export Controls Begins in the EU: The Revised EU Dual-Use Export Controls to Promote Human Rights", *SheppardMullin,* May 14, 2021, *https://www.globaltradelawblog.com/2021/05/14/dual-use-export-controls-promote-human-rights/.*

124 Daniel Moßbrucker, "EU States Unanimously Vote Against Stricter Export Controls for Surveillance Equipment," Netzpolitik.org, (Berlin, Germany), July 16, 2019, https://netzpolitik.org/2019/eu-states-unanimously-vote-against-stricter-export-controls-for-surveillence-equipment/; Daniel Moßbrucker, "Surveillance Exports: How EU Member States Are Compromising New Human Rights Standards," Netzpolitik.org, (Berlin, Germany), October 29, 2018, https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/; Patrick Howell O'Neill, "Inside NSO, Israel's Billion-Dollar Spyware Giant," *MIT Technology Review*, August 19, 2020, https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/.

125 Declaration of Shalev Hulio In Support of Defendants' Motion to Dismiss, WhatsApp Inc. v. NSO Group Technologies Limited, 2 April 2020, paras. 5-9, 12, www.courtlistener.com/docket/16395340/45/11/whatsapp-inc-v-nso-group-technologies-limited/; Statement disseminated by Mercury Public Affairs, LLC, on behalf of Q Cyber Technologies Ltd., NSD/FARA Registration Unit, 2 October 2020, https://efile.fara.gov/docs/6170-Informational-Materials-20201002-729.pdf.

126 Kali Robinson, "How Israel's Spyware Stoked Surveillance Debate," *Council on Foreign Relations,* March 8, 2022, https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.

127 "Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," United Nations General Assembly, May 28, 2019, https://documents.un.org/doc/undoc/gen/g19/148/76/pdf/g1914876.pdf?token=ILbcRnDnfZ18fonWDP&fe=true.

Export licensing regimes can act as a legal mechanism to collect vendor records and some limited activity data. This recommendation suggests strengthening them for that purpose in three ways.

First, export control licenses for spyware and closely related services should include the names of all employees whose work has a material impact on the development of the product subject to the export license. This is important information for policymakers on two grounds. First, these employees are tied to a specific product or spyware service in a semi-public record in perpetuity. This may have some deterrent effect in choosing to work with these registered vendors and stops short of lifetime bans or similar sanctions. The record serves as an indicator of behavior at a certain point in time but does not constitute a lifetime scarlet letter. Second, these companies are tied to those employees, also at a point in time. The sample of the spyware market captured in this dataset has shown vendor names and labels to be a fluid construct and policies should be focused on learning, and potentially shaping, the behavior of individuals in this market more directly. Should a vendor seek to shift jurisdiction and apply for appropriate export licenses for the same product in their new domicile, embedded "critical employee" information in these licenses would ensure a paper trail.

The determination of what constitutes material impact, as well as defining covered products beyond the language in the Wassenaar Arrangement, would need to be determined by each county at the national level. In the US, this should come from a Bureau of Industry and Security (BIS) policy guidance. Under the Department of Commerce, BIS is already "actively engaged in formulating, coordinating, and implementing various export controls to counter the use of items subject to the Export Administration Regulations (EAR) that could enable human rights abuses or repression of democracy throughout the world."[128] More widely, this would inform a working group under the continuing Joint Statement mechanism as the seventeen signatories seek to harmonize their definitions and enforcement of this additional requirement.

Second, to ensure export controls are effective domestically, governments should build mandatory and regular audits into licensure practices along with punishments for non-compliance. In the United States, the BIS is responsible for regulating the export of dual-use products and services under EAR, including the Commerce Control List of Dual-Use Items (CCL). BIS's Export Compliance Guidelines contain a section on audits with broad guidelines for auditors, but poor execution or a lack of audits is a recurring barrier in the implementation of EAR.[129]

An export license for software should also include an explicitly time-bound permission to export. The concept of "continuous monitoring" is an approach to security and compliance in cybersecurity that acknowledges software cannot be evaluated and "signed off" on at a single point in time, but rather needs to be continuously tracked throughout its operation. The same is true of the spyware vendor business model and regular audits of these licenses would accomplish much the same ends. The auditing process, conducted by the licensing authority with appropriate specialized support, would enhance transparency in the export control process and allow licenses to be revoked in the face of evidence of abuse or misuse of spyware vendors' products. An effective audit would scrutinize all aspects of an export licensing process including application procedures, decision-making criteria, approval processes, monitoring mechanisms, and compliance enforcement. In this way, any discrepancies or red flags discovered could be disclosed to partner agencies to execute audit recommendations.[130]

Third, these audit reports and the original export licenses should also be made accessible to the public by the national licensing authority; this would be BIS in the case of the US. Reasonable redaction of personally identifiable or business-sensitive information could be made but this should be weighed heavily against the significant public interest in greater transparency in the activities of spyware vendors. Public export license records would complement largely private KYV data and allow for the broader research and civil society community to fulfill an important role as external accountability mechanisms.

Export controls are, at best, a marginal utility in regulating the spyware market. Their focus on transactions emphasizes one of the least regulable steps in the spyware supply chain and to expect licensing to address myriad end uses or all facets of vendor behavior would be wildly optimistic. Instead, this recommendation proposes to take export licensing for the marginal benefit it might offer policymakers and deriving additional value from improved transparency—without leaving export controls as the sole, or even most critical, line of defense against the risks of spyware.

128 "Promoting Human Rights and Democracy," *Bureau of Industry and Security, U.S. Department of Commerce,* Accessed July 28, 2024, https://www.bis.doc.gov/index.php/human-rights.

129 15 C.F.R. §§ 730–780, "Subchapter C: Export Administration Regulations," https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C; "Export Compliance Guidelines: The Elements of an Effective Export Compliance Program," US Department of Commerce: Bureau of Industry and Security, n.d., https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file.

130 "Red Flag Indicators," US Department of Commerce: Bureau of Industry and Security, accessed July 11, 2024, https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators.

4. Limit jurisdictional arbitrage by vendors

Imposing policy outside of a state's jurisdiction is challenging and presents opportunities for spyware vendors and others seeking to elude regulatory controls. This extraterritoriality is often exploited by spyware vendors to engage in jurisdictional arbitrage and take advantage of inconsistencies across governments. This recommendation outlines several steps to limit this arbitrage, focusing on raising the barrier for vendors associated with an export license for electronic surveillance technologies, including spyware, to leave a single jurisdiction and mandate reporting of new branches and subsidiaries. To keep things simple, this recommendation defines surveillance technologies using the State Department's language from the Joint Statement: "Technologies used for surveillance can refer to products or services that can be used to detect, monitor, intercept, collect, exploit, preserve, process, analyze, invasively observe, and/or retain sensitive data, personally identifying information, including biomarkers, or communications concerning individuals or groups."[131]

Jurisdictional arbitrage by spyware vendors undermines the rule of law, efficiency of regulatory supervision, and market integrity, and can trigger regulatory competition amongst different jurisdictions where states adopt low-standard regulatory requirements to attract business and investments.[132] For example, the European Union, theoretically, has strong regulations against spyware vendors including Council Regulation (EC) No. 2021/821 which ensures regulatory consistency across EU member states.[133] However, the bloc faces fragmentation when it comes to implementation with countries like Bulgaria, Cyprus, Greece, Italy, Malta, and Hungary demonstrating highly variable political commitment to or institutional capacity for strict export controls.[134] Intellexa is a prime example of a vendor that established new subsidiaries in these countries to take advantage of jurisdictional arbitrage.[135]

To address this problem, policymakers should first make it more challenging and costly for a vendor with an export license to exit a jurisdiction. This should include mandating the public disclosure of any subsidiary or branch openings or closures by a vendor that has been granted a license to export spyware. Second, policymakers with existing authorities to regulate inbound investment (such as the Committee on Foreign Investment in the United States–CFIUS) should automatically review transactions impacting the ownership structure of domestic spyware vendors in any way. Vendors that fail to flag such transactions (such information may come to light in mandated KYV disclosures, for instance) should be barred from participating in government acquisitions and/or have their export licenses suspended for some period.

Consider the example of the disclosure requirements of the banks which are members of the Federal Reserve System in the United States.[136] These banks are required by the Federal Deposit Insurance Act to seek approval of and disclose to the Federal Reserve (as well as the public) any instances of openings, closures, or mergers with another bank, including the closure of any bank branches as a result of mergers and acquisitions.[137] This requirement ensures that the Federal Reserve can monitor and supervise the geographical footprint and operational changes of banks across different states and regions.[138] In the context of the spyware market, a notification requirement would enhance the transparency of the market and help put regulators in different jurisdictions on a more equal footing. It would also allow key stakeholders, including civil society organizations, to have visibility into the operations of spyware vendors and their compliance with regulatory requirements.

131 "The Guiding Principles on Government Use of Surveillance Technologies," *U.S. Department of State,* March 30, 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/; and the commitments made as part of the "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", *The White House,* March 18, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

132 Danièle Nouy, "Gaming the Rules or Ruling the Game? – How to Deal with Regulatory Arbitrage" (Speech by Nouy, as Chair of the Supervisory Board of the ECB, at the 33rd SUERF Colloquium, Helsinki), September 15, 2017, European Central Bank, https://www.bankingsupervision.europa.eu/press/speeches/date/2017/html/ssm.sp170915.en.html; Janet Dine, "Jurisdictional Arbitrage by Multinational Companies: A National Law Solution?" *Journal of Human Rights and the Environment* 3, no. 1 (March 2012): 44–69, https://doi.org/10.4337/jhre.2012.01.02; Sideris Draganidis, "Jurisdictional Arbitrage: Combatting an Inevitable by-Product of Cryptoasset Regulation," *Journal of Financial Regulation and Compliance* 31, no. 2 (March 29, 2023): 170–85, https://doi.org/10.1108/JFRC-02-2022-0013.

133 "Regulation (EU) 2021/821"; "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)," *Official Journal of the European Union* (Luxembourg: Publications Office of the European Union, May 5, 2009), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428.

134 Omtzigt, "Pegasus and Similar Spyware and Secret State Surveillance."

135 Omtzigt, "Pegasus and Similar Spyware and Secret State Surveillance."

136 "eCFR :: 12 CFR Part 208 -- Membership of State Banking Institutions in the Federal Reserve System (Regulation H)," accessed July 30, 2024, https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-208.

137 "Supporting Statement for the Domestic Branch Application (FR 4001; OMB No. 7100-0097)," n.d., https://www.federalreserve.gov/reportforms/formsreview/FR%204001%20OMB%20SS.pdf.; "Electronic Applications and Applications Filing Information–State Member Bank," Board of Governors of the Federal Reserve System, accessed July 31, 2024, https://www.federalreserve.gov/supervisionreg/afi/smfilings.htm.; "12 U.S.C. 1831r-1 - Notice of Branch Closure - Document in Context - USCODE-2010-Title12-Chap16-Sec1831r-1," accessed July 31, 2024, https://www.govinfo.gov/app/details/USCODE-2010-title12/USCODE-2010-title12-chap16-sec1831r-1/context.

138 "Compliance Handbook," *Federal Reserve*, n.d., https://www.federalreserve.gov/boarddocs/supmanual/cch/closings.pdf.

Third, harmonizing these disclosure requirements should be the subject of another working group under the Joint Statement or a similar collaborative mechanism. Effective barriers to market exit by these spyware vendors would help to improve the potential influence of domestic policies, including those across the EU, on these firms. Consistency in those barriers would reduce the incentives toward arbitrage.

5. Provide greater protection against Strategic Lawsuits Against Public Participation (SLAPP)

One of the abiding trends of this research and the work of the broader analytic community examining spyware is the tremendous importance of open reporting. There is no substitute for applied public policy analysis in this space but the relationship between journalism and research is deeply symbiotic. A disturbing recent trend threatens to undermine this reporting as a handful of spyware vendors deploy Strategic Lawsuits Against Public Participation (SLAPP).[139]

In 2022, the news outlet Reuters was sued for defamation against a vendor's parent company profiled in this report, Appin Technologies and Appin Security Group. As a result, Reuters removed an investigation into the group's activities from its website.[140] This lawsuit sets a dangerous precedent for journalists and researchers alike who offer much-needed transparency into an already opaque market.

To address the harms and frequency of SLAPP suits more generally, the European Commission established a set of rules in May of 2024 that provide heightened protections for speech on matters of "public interest."[141] The essential elements of these rules would be a suitable starting point for comparable policies in the United States and elsewhere, including:

a) Accelerated treatment of issues raised under these heightened protections.

b) The possibility for early dismissal of "claims against public participation" which are determined to be "manifestly unfounded" at "the earliest possible stage in the proceedings, in accordance with national law."

c) Provision for the recovery of all costs of the proceedings by defendants and the potential for application of "effective, proportionate and dissuasive penalties or other equally effective appropriate measures, including the payment of compensation for damage or the publication of the court decision" on the party initiating the action.[142]

It would also be welcome for states that host the victims of SLAPP suits to raise the issue through existing diplomatic channels with states hosting parties initiating these suits. In practical terms, the State Department should address the impact of the Appin suit against Reuters with the Indian and UK governments (as the domicile of the claimant vendor and the court of jurisdiction respectively). This does little to impact the suit directly but shows awareness by the US government and may raise the costs of action by firms in these countries.

139 For more on anti-SLAPP laws and related resources, see an excellent resource from the Reporters Committee for Freedom of the Press titled "Understanding Anti-SLAPP Laws," available at: https://www.rcfp.org/resources/anti-slapp-laws/.

140 "Editor's Note," *Reuters,* December 5, 2023, https://www.reuters.com/investigates/special-report/usa-hackers-appin/.

141 "Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings ('Strategic lawsuits against public participation'), *Official Journal of the European Union,* April 11, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024L1069.

142 Hat tip to Lisandra Novo for this excellent suggestion.

AREAS FOR FUTURE WORK

These recommendations focus on achieving greater transparency across the spyware market, limiting jurisdictional arbitrage by vendors, and more effectively scrutinizing supplier and investor relationships with those vendors. They do not address the full range of issues that urgently need greater attention and resolution in the proliferation of spyware. This section addresses these opportunities for future work and concludes with a call for consensus and action by at least a small group of states to advance these and related policies.

Future Work

Bringing the brokers back in: There is insufficient coverage of supplier firms in this dataset relative to the number of spyware vendors. These firms, some of which might be categorized as exploit "brokers," are important to the discussion of how to reduce the harms associated with spyware, but they are less widely reported on and not systematically understood. These firms traffic in information, and to some degree talent, whose product is not intrinsically malicious (and which has been subject to poorly conceived controls in the past). At the same time, the activities of these suppliers and brokers are a critical wedge between advocates for more effective spyware policy rooted in national security concerns and those advocating from a human rights-centered perspective (acknowledging a degree of overlap between the two). Better information on the diversity of locations, activities, and organization of these firms would benefit an otherwise opaque segment of this market whose activities extend far beyond spyware. The length of supply chains across the spyware market, and the number of steps between suppliers for high-risk vendors as well as governments otherwise practicing adequate due diligence against abuse, could be a substantial driver of unaddressed risk and merits further investigation.

Spyware vendors or suppliers partnered with major tech firms: There are several instances where spyware vendors or suppliers have formed partnerships with conventional technology firms. Positive Technologies may be the most notable, having previously been a member of Microsoft's Active Protections Program (MAPP) and publicly advertising its work with Samsung.[143] The structure of these relationships may be tied to vulnerability disclosure, underlining the complex role played by vulnerability discovery and exploitation in both offensive and defensive activities.

A "who's who" for spyware investors: The incentives for different kinds of investors (for example, venture capital firms vs. private equity) are clear in conventional markets, but much less so in the spyware sector. Both types of entities appear in this dataset. Designing a more robust due diligence regime for investors in these vendors would benefit from a more precise understanding of the motivations of different types of investors for entering the market.

The customer might often be wrong: This project has not yet covered the range of government customers to which this market largely caters. The behavior of these agencies, parties, offices, and bureaus should be of significant interest as they are the ultimate source of demand that shapes the spyware market. States willing to take affirmative action against the spyware market may also quickly find they have better existing tools to shape the behavior of their allies and partners, integrating spyware into wider defense assistance, trade, and legal cooperation agendas. Cataloging customers, their relationships with specific firms and associated supply chains, and the timing of these relationships is a fruitful area for future work. How those customer relationships form and their portability between spyware vendors is also worth continued analysis.

A role for technology companies: Technology firms have a role to play in shaping the spyware market, if for no other reason than they may be supplying Software-as-a-Service (SaaS) and other technologies to spyware-related firms. Research from Amnesty International and others in 2021 established the NSO Group was using AWS products as part of the command-and-control infrastructure for its spyware product and even earlier reporting from Motherboard pointed to NSO delivering its product from an Amazon IP address.[144] Discovery as part of an ongoing lawsuit between Meta and NSO established that NSO became an AWS customer beginning in 2018.[145]

Technology companies might play at least two roles in further shaping the spyware market. First is executing due diligence on technology sales, especially export-controlled

143 Ionut Arghire, "Russian Security Vendor Positive Technologies Dropped From MAPP Member List," Security Week, April 19, 2021, https://www.securityweek.com/russian-security-vendor-positive-technologies-responds-us-sanctions/; "Spotlight / China, Russia: Huawei Hired Top Researchers from Russia's US-Sanctioned NeoBit," Intelligence Online, June 18, 2021, https://www.intelligenceonline.com/corporate-intelligence/2021/06/18/huawei-hired-top-researchers-from-russia-s-us-sanctioned-neobit,109674074-eve.

144 "Forensic Methodology Report: How to catch NSO Group's Pegasus," Amnesty International, July 18, 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/; Joseph Coz, "Forensic Methodology Report: How to catch NSO Group's Pegasus," Vice/Motherboard, May 20, 2020 https://www.vice.com/en/article/qj4p3w/nso-group-hack-fake-facebook-domain.

145 Suzanne Smalley, "WhatsApp: AWS leased infrastructure to NSO Group beginning in 2018," The Record, March 17, 2024, https://therecord.media/aws-leased-infrastructure-nso-pegasus-whatsapp-lawsuit.

hardware and cloud services over a certain dollar threshold, to determine if the customer is an identified participant in the spyware market. Those identified customers should be subject to scrutiny and possible removal but early identification would help cloud vendors avoid discovering via the media that their services are being used in the development or deployment of spyware. Second is major technology firms, perhaps only cloud service providers, developing a common code of conduct as to how they sell services to participants in the spyware market and under what conditions they might limit or refuse sales. The development of both this review policy and the code of conduct are prospects for future work. In the meantime, major technology companies like Meta, Apple, Google, and Microsoft remain some of the only entities with both the standing *and* the resources to conduct sustained legal action against vendors selling products that create significant risk or harm.

Whistleblowers: While open reporting and journalism are important sources of transparency in this market and deserve heightened protection, the status of whistleblowers from spyware vendors or customers is uncertain. Consolidated guidance as to the human rights or procedural responsibilities of spyware vendors and their customers, accounting for jurisdiction, would help to clarify under what conditions an employee or government official might act with adequate legal protections. Specifying the kinds of legal or ethical expectations of vendors and customers, as well as clarifying protections both against retaliation and to navigate limits on publishing proprietary information, at a national level, would help strengthen an important channel of information on the use and abuse of these products.

Clarifying de-listing procedures: An important feature of an effective sanctions regime is a transparent de-listing procedure.[146] Given the purpose of imposing sanctions is to cause behavior change in the sanctioned entity or individual, sanctioned entities and individuals should be able to request de-listing once they have demonstrably changed their practices. This is important for ensuring the legitimacy and credibility of sanctions regimes. Hence, governments and multilateral organizations should clearly specify the process and conditions that result in the de-listing from their sanctions list and both researchers and advocates can help map out these processes.

What comes next: How do these and other proposed changes impact the shape and jurisdictional concentration of the spyware market? One of the risks for more assertive regulation of spyware development, sales, and use is vendors, suppliers, or other entities moving to jurisdictions outside the reach of those states using policy to shape this market. The suggestion is not unwarranted in no small part because of the jurisdictional arbitrage already observed in this market. More work is needed to understand what policies might pose the greatest likelihood of this market shift or its segmentation into multiple tiers. This dataset (a sample of the market) shows that even vendors in "hard to reach" jurisdictions with local governments unwilling to regulate their behavior still rely on foreign capital and suppliers. These investors and suppliers are often based in states with a demonstrated willingness to enforce existing policies on spyware. Therein lies the opportunity for change.

146 "Best Practices for the Effective Implementation of Restrictive Measures," (Brussels, Belgium: General Secretariat of the Council of the European Union, June 27, 2022), https://data.consilium.europa.eu/doc/document/ST-10572-2022-INIT/en/pdf.

CONCLUSION

There is a certain macabre humor in the lengths that spyware firms go to in obscuring their true nature and purpose, disguising themselves as mythical beasts in an obscured global market. The purpose of this report is primarily to demystify—or *demythify*—the global spyware market, moving beyond coverage of individual firms to unveil a network of relationships between spyware vendors, suppliers, and investors across forty-two different countries. This data is only a sample but it evidences several trends, including cross-border financial support, shifting vendor identities, and a pattern of jurisdictional arbitrage which would undermine discrete national-level efforts to reshape this market. There is more to be discovered about this market and the authors' sincere hope is that this project provides support to many other researchers, analysts, and advocates.

Policies that work to regulate and influence the spyware market, which are coordinated amongst at least a small set of countries, have better prospects to reduce the harms and risks posed by spyware. Policymakers who succeed at improving transparency in this market, raising barriers to vendor reorganization and reincorporation, and applying greater scrutiny on supplier and investor relationships will directly confront critical drivers of spyware's proliferation and abuse. The recommendations presented in this report address these three priorities while laying the groundwork for granular controls on transactions and policies based on distinctions in the legitimate use of spyware.

Most available evidence suggests that spyware sales are a present reality and likely to continue. Proliferation heedless of its potential human rights harms and national security risks, however, is not a stable status quo. Little of the present market for spyware is regulated or governed well enough to address these harms and risks. In some areas, there is a pressing need for additional research but in many others, the initiative sits with policymakers. Nascent steps by a handful of countries demonstrate that a more vigorous approach to shape the behavior of spyware vendors, their supply chain, and their investors is possible. Where such progress has been stymied by a lack of systematic data on this market, Mythical Beasts offers a contribution. However, much more remains to be done.

ACKNOWLEDGMENTS

Mythical Beasts was made possible with the support of Microsoft and the UK's National Cyber Security Centre, we extend sincere thanks to the teams in Redmond and London for their commitment to this work. This project owes a debt of gratitude to the security research community, in particular Sophia d'Antoine, and contributors both inside and out of the Cyber Statecraft network for early conversations that helped shape this research. Thank you to Kirsten Hazelrig, James Shires, and several others who wish to remain anonymous. For peer review of this report, the dataset, and its interactive, thank you to Chris Delaney, Kaja Ciglic, John Hering, David Agranovich, Ingrid Dickinson, Emma Schroeder, Jorn Fleck, Clement Lecigne, Salo Aburto, Jessica Dabrowsky, James Batchik, Constantine Stasinopoulos, Jennifer Brody, Kimberly Donovan, and Lisandra Novo.

Thank you to Stewart Scott and Alexander Beatty for their contributions which early on shaped the focus of this report and perspectives on its art. Thank you to Nancy Messieh for all the graphics and to the team at Schema Design for the interactive version of this dataset. Thanks and appreciation are due to Andrey Prokopenko for the artwork and for his creative output despite terrific challenges. Major credit to Emma Taylor as well as Jean Le Roux and Sopo Gelava without whose collaboration the dataset and its presentation would not have been possible. Thank you to Natalie McEvoy, Charlette Goth-Sosa, Kristopher Kaliher, and Donald Partyka for review, editing, and production. For feedback on this project as it evolved thank you as well to the attendees of more than half a dozen roundtables and events over the past year and to the members of two different communities for your time, questions, and willingness to engage.

APPENDICES

Appendix A — Supplier and Vendor Profiles

This appendix summarizes the profiles of suppliers and vendors within the dataset that are included in the analysis of this report. The authors sought to include this information to outline details about all entities within the dataset.

SUPPLIERS

Azimuth Security

In 2010, Mark Dowd and John McDonald founded Azimuth Security, an Australia-based exploit developer and boutique hacking firm.[147] The company gained notoriety for its role in unlocking the San Bernadino shooter's iPhone in 2016. In 2018, an American firm, L3 Technologies, now L3Harris, purchased Azimuth Security and Linchpin Labs of Canada.[148] Today, Azimuth and Linchpin Labs operate under the brand name "Trenchant." The Trenchant group of companies operates across three jurisdictions: United Kingdom, Canada, and Australia. L3Harris Trenchant Trenchant Canada Inc. (Canada), and Australia.[149] In the past, Azimuth supposedly restricted sales to members of the Five Eyes intelligence alliance—Australia, Canada, New Zealand, the United Kingdom, and the United States.[150] Trenchant does not currently face any restrictions to its exploit sales or business operations.

Blue Oceans Technologies

Blue Ocean Technologies is an Israeli supplier that was incorporated in 2015[151] by retired Brigadier General Rami Ben Efraim and Lieutenant Colonel Ron Tira.[152] An Israeli newspaper, *The Globes*, reported that Blue Ocean Technologies is an exception in the Israeli spyware market since it was established as part of a deal between an East Asian country and the founders of the firm.[153] Intelligence Online claims that the East Asian country is Singapore, and Blue Ocean Technologies received two export licenses from the Israeli Defense Ministry to provide the Singaporean Ministry of Defense with a team of vulnerability researchers to weaponize Singapore's cyber tools.[154]

Brigadier General Rami Ben Efraim, through his strategic consulting firm Lee and Rami Ben-Efraim Ltd. (also known as BNF Group), holds options in Blue Ocean Technologies.

Computer Security Initiative Consultancy PTE Ltd. (COSEINC)

Founded in 2004 in Singapore,[155] Computer Security Initiative Consultancy PTE Ltd. (known widely as COSEINC) is known for distributing exploits without control and known to host pwn0rama—its own cyber vulnerability acquisition program[156]—and is classified as a supplier within this dataset. The Bureau of Industry and Security (BIS) of the US Department of Commerce added COSEINC to its Entity List for Malicious Cyber Activities in November 2021 based on a BIS determination that the vendor "traffic[s] in cyber tools used to gain unauthorized access to information systems,

147 "L3HARRIS AZIMUTH SECURITY PTY. LIMITED ACN 141 714 061," Australian Securities and Investments Commission (ASIC), accessed July 3, 2024, https://connectonline.asic.gov.au/RegistrySearch/faces/landing/panelSearch.jspx?_adf.ctrl-state=fkb9ywzcb_15&searchText=141714061&searchType=OrgAndBusNm; "The Team," Azimuth Security, accessed July 3, 2024, https://www.azimuthsecurity.com/theteam.

148 Jane Edwards, "L3 to Buy Cyber Firms Linchpin Labs, Azimuth Security for $200M; Christopher Kubasik Comments," GovCon Wire, July 12, 2018, https://www.govconwire.com/2018/07/l3-to-buy-cyber-firms-linchpin-labs-azimuth-security-for-200m-christopher-kubasik-comments/.

149 "L3Harris Trenchant Canada Inc (Company Profile)," OpenCorporates, accessed July 3, 2024, https://opencorporates.com/companies/ca/7056401; "L3HARRIS TRENCHANT LTD – United Kingdom (Company Profile)," OpenCorporates, accessed July 3, 2024, https://opencorporates.com/companies/gb/09068202; "L3HARRIS AZIMUTH SECURITY PTY. LIMITED ACN 141 714 061," ASIC.

150 Joseph Cox and Lorenzo Franceschi-Bicchierai, "How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of," Vice (blog), February 7, 2018, https://www.vice.com/en/article/8xdayg/iphone-zero-days-inside-azimuth-security.

151 This is based on the records from the Israeli Corporate Authority (see also: "Blueocean Technologies Ltd., Petah Tikva, Israel (Company Profile)," North Data, accessed July 3, 2024, https://www.northdata.com/Blueocean+Technologies+Ltd.,+Petah+Tikva/ICA-515223196). However, the authors would like to note that there is at least one other source that claims that Blue Ocean Technologies was incorporated in 2017 (see: Assaf Gilead, "Israeli Cyberattack Co Blue Ocean Serves East Asian Gov't," *Globes*, May 14, 2023, https://en.globes.co.il/en/article-israeli-cyberattack-co-blue-ocean-serves-east-asian-govt-1001446311).

152 "Israel: Rami Ben Efraim Adds Planet Nine to Growing Cyber Empire," Intelligence Online, December 21, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/12/21/rami-ben-efraim-adds-planet-nine-to-growing-cyber-empire,110131613-art.

153 Assaf Gilad, "Air Force Veterans Founded a Cyber Offensive Company for a Foreign Country," *Globes*, December 5, 2023, https://www.globes.co.il/news/article.aspx?did=1001446258.

154 "Israel: Cyberintelligence Firm Blue Ocean's Mystery Clients Revealed," Intelligence Online, May 30, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/05/30/cyberintelligence-firm-blue-ocean-s-mystery-clients-revealed,109978498-art.

155 "COSEINC (Company Profile)," Crunchbase, accessed July 3, 2024, https://www.crunchbase.com/organization/coseinc.

156 "China, Singapore, United States: Blacklisted by the US, Zero Day Distributor COSEINC Works on for China's Pwnzen," Intelligence Online, November 8, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/11/08/blacklisted-by-the-us-zero-day-distributor-coseinc-works-on-for-china-s-pwnzen,109703349-art.

threatening the privacy and security of individuals and organizations worldwide."[157]

COSEINC was founded by Thomas Lim, who is known for organizing a security conference, SyScan, until it was sold to Chinese technology firm Qihoo 360, another sanctioned entity.[158] In 2015, WikiLeaks exposed Lim's attempt to sell hacking tools to Italian Spyware vendor Hacking Team srl,[159] thereby, hinting at a possible connection between COSEINC and Hacking Team srl.[160] In 2022, the company became inactive.[161]

Crowdfense Technological Project Management - Sole Proprietorship LLC

Founded in 2017 in the United Arab Emirates (UAE), Crowdfense Limited buys, develops, and sells zero-day exploits that target a variety of platforms. In 2018, Crowdfense Limited launched its first bug bounty program with a $10 million budget.[162] Since then, the company has continued to grow its bug-bounty budget year over year as it expands the scope of its "interest" areas. According to the UAE business registry, Crowdfense Limited dissolved in 2023 and a new entity named Crowdfense Technological Project Management - Sole Proprietorship LLC was registered. In 2024, Crowdfense Technological Project Management-Sole Proprietorship LLC boasted a $30 million budget that now includes exploit acquisitions related to "Enterprise Software, WiFi/Baseband and Messengers."[163] The company maintains an unknown number of offices in Abu Dhabi[164] and some reporting indicates it receives financial backing from the governments of the UAE and Saudi Arabia.[165]

Dataflow Security s.r.l.

DataFlow Security s.r.l. (AKA DFSEC) was founded in 2022 by Ofer Cohen.[166] Based in Italy, the company specializes in vulnerability research and exploit development.[167] This report classifies DFSEC as a supplier due to its development, optimization, and sale of exploits. DFSEC's internal client website contains a catalog of exploits for purchase. In 2022, Dataflow Security Spain SL was established in Spain.[168] In the same year, Dataflow Forensics was established as a sister company to DFSEC focused on defensive cybersecurity operations.[169] DFSEC acquired a majority stake in Random Research, an Israeli company also founded by Ofer Cohen.[170] At this time, there is little available information concerning DFSEC funding. However, per the official Spanish corporate gazette, the sole shareholder of Dataflow Security Spain SL is Dataflow Security s.r.l., and while there has been no update to the company's shareholders since its incorporation its share capital increased from 3,000 Euros to 153,000 Euros on June 28, 2024.[171] This commonly indicates a new investment and/or a new shareholder. However, limited companies are not required to declare shareholders in the Spanish public gazette. This group of firms has not faced any significant roadblocks to business operations.

157 "Commerce Adds NSO GRoup and Other Foreign Companies to Entity List for Malicious Cyber Activities," U.S. Department of Commerce, Accessed July 28, 2024, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

158 "Addition of Entities to the Entity List, Revision of Certain Entries on the Entity List (A Rule by the Industry and Security Bureau)," *Federal Register*, June 5, 2020, https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list.

159 "Re: 0 days," WikiLeaks (Hacking Team Archive), accessed July 3, 2024, https://wikileaks.org/hackingteam/emails/emailid/695766.

160 Tsyrklevich, "Hacking Team: A Zero-Day Market Case Study."

161 "OpenCorporates: The Open Database of The Corporate World," accessed July 3, 2024. https://opencorporates.com/events/2762512532.

162 Crowdfense, "Crowdfense Launches $10 Million Bug Bounty Program," PR Newswire, April 24, 2018, https://www.prnewswire.com/news-releases/crowdfense-launches-10-million-bug-bounty-program-300635496.html.

163 "About Us - Crowdfense." n.d. Accessed July 3, 2024. https://www.crowdfense.com/about-us/.

164 ITP Staff, "Crowdfense to Expand Scope and Funding for Bug Bounty Program," *Edge*, December 9, 2018, https://www.edgemiddleeast.com/services/618451-crowdfense-to-expand-scope-and-funding-for-bug-bounty-program.

165 "Singapore, UAE: Emerging SIGINT Powers Seek Own Cyber-Bounty Hunters," Intelligence Online, May 16, 018, https://www.intelligenceonline.com/international-dealmaking/2018/05/16/emerging-sigint-powers-seek-own-cyber-bounty-hunters,108310461-art.

166 "Dataflow Security – Defining the Forefront of Innovation, Mastering Vulnerability Research," accessed July 3, 2024, https://dfsec.com/; "Ofer Cohen – Founder at Dataflow Security (Organization Chart)," The Org, accessed July 3, 2024, https://theorg.com/org/dataflow-security/org-chart/ofer-cohen.

167 "Dataflow Security – Defining the Forefront"; "Dataflow Security Spain SL, Madrid, Spain (Company Profile)," North Data, accessed July 3, 2024, https://www.northdata.com/Dataflow+Security+Spain+SL,+Madrid/NIF+B10866671.

168 "Dataflow Security Spain SL, Madrid, Spain."

169 "DATAFLOW FORENSICS INC. (Company Profile)," OpenCorporates," accessed July 3, 2024, https://opencorporates.com/companies/us_ny/6616280; "Dataflow Security – Defining the Forefront"; "Italy, United States: Dataflow Security Sets up New Forensics Company in New York," Intelligence Online, October 27, 2022, https://www.intelligenceonline.com/surveillance--interception/2022/10/27/dataflow-security-sets-up-new-forensics-company-in-new-york,109839003-art.

170 "מ"עב רקחמ מודנר (Company Profile)," [alternative legal name: Random Research], OpenCorporates, accessed July 3, 2024, https://opencorporates.com/companies/il/516847472; "The Tech Times: Assured Information Security's Cyber Contract Renewed, Ofer Cohen Launches Israeli Firm, Brian Katz into Private Sector," Intelligence Online, November 2, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/11/02/assured-information-security-s-cyber-contract-renewed-ofer-cohen-launches-israeli-firm-brian-katz-into-private-sector,110083925-art.

171 *BOLETÍN OFICIAL DEL REGISTRO MERCANTIL* SECCIÓN PRIMERA Empresarios Actos inscritos MADRID, June 5, 2024, https://www.boe.es/borme/dias/2024/07/05/pdfs/BORME-A-2024-129-28.pdf.

PARS Defense

Registered in Turkey in 2021, PARS Defense was founded by Ibraham Baliç, an individual who has been operating as a "vulnerability specialist" since 2010.[172] PARS Defense specializes in detecting vulnerabilities and operating codes on mobile systems and is coded as a supplier within the dataset. Google identified two vulnerabilities attributed to PARS defense that were present in iOS.[173]

No information was found on PARS Defense subsidiaries, partners, holding companies, or investors.

Protect Electronic Systems LLC

Founded in 2016, Protect Electronic Systems LLC, also known as Protect and Protected AE, is a supplier based in the United Arab Emirates.[174] The company was reportedly founded from what remained of DarkMatter's zero-day exploit.[175] More recently, Protect Electronic Systems received attention due to its "special relationship" with Variston IT, a vendor tracked in this report.[176] Protect Electronic Systems built upon Variston spyware's "framework and infrastructure" to create a polished product to sell directly to brokers and governments.[177] At this time, little is known regarding Protect Electronic Systems' investor base; however, some sources indicate the company may receive state funding.

RebSec Solutions

RebSec Solutions was incorporated in 2012 by Vishvadeep Singh in India and is classified as a supplier within this dataset. It was not possible to identify any institutional or angel investors in RebSec Solutions but the quality of data in open reporting on this firm is limited.[178]

Zerodium LLC

In 2015, Chaouki Bekrar founded Zerodium LLC in the United States. Bekrar previously founded and led Vupen, a French zero-day exploit vendor. Vupen clients reportedly included "vetted" NATO government agencies, specifically the US National Security Agency (NSA).[179] After Vupen dissolved in 2015, Zerodium LLC emerged to provide identical services in the zero-day exploit industry.[180] Vista Incorporations Limited is Zerodium LLC's registered agent in Delaware.[181] Amidst a market typically shrouded in financial mystery, Zerodium LLC was one of the first firms to put out ads detailing desired exploit specifications with corresponding prices.[182] Other companies, including Russia's OpZero, Have followed suit and adopted similar public marketing strategies.[183] Currently, Zerodium LCC is a privately held venture capital-backed company; however, little information exists concerning the company's investor base.[184]

172 "Turkey: Pars Defense, Turkey's Zero-Day Champion," Intelligence Online, February 15, 2024. https://www.intelligenceonline.com/surveillance--interception/2024/02/15/pars-defense-turkey-s-zero-day-champion,110159845-art; Graham Cluley, "Was Ibrahim Balic the Man Who 'Hacked' Apple's Developer Center?" (author blog), July 22, 2013, https://grahamcluley.com/was-this-the-man-who-hacked-apples-developer-center/.

173 Shubham Bhandari, "Google Links Over 60 Zero-Days to Commercial Spyware Vendors," LinkedIn (post), February 7, 2024, https://www.linkedin.com/pulse/google-links-over-60-zero-days-commercial-spyware-vendors-bhandari-oxvnc/.

174 "UAE: Abu Dhabi's Protect Takes over DarkMatter's Cyber-Offensive Role," Intelligence Online, May 27, 2019, https://www.intelligenceonline.com/international-dealmaking/2019/05/27/abu-dhabi-s-protect-takes-over-darkmatter-s-cyber-offensive-role,108358798-art; "Buying Spying: Insights into Commercial Surveillance Vendors," Google, February 2024, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.

175 "UAE: Digital14 Picks up Darkmatter's Key Activities, Including the Vulnerabilities Researcher xen1thLabs," Intelligence Online, January 21, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/01/21/digital14-picks-up-darkmatter-s-key-activities-including-the-vulnerabilities-researcher-xen1thlabs,109636378-gra.

176 Lorenzo Franceschi-Bicchierai, "Spyware Startup Variston May Be Shutting Down," Techcrunch, Business & Human Rights Resource Centre, February 15, 2024, https://www.business-humanrights.org/en/latest-news/spyware-startup-variston-may-be-shutting-down/.

177 "Buying Spying."

178 "Rebsec Solutions Company Profile (Overview)," Tracxn, accessed June 12, 2024, https://tracxn.com/d/companies/rebsec-solutions/__fwWI5NbcY9wydDJGa_LhP1Fo0thK_R070rY_RyUH1BE.

179 Andy Greenberg, "Meet The Hackers Who Sell Spies the Tools To Crack Your PC (And Get Paid Six-Figure Fees)," *Forbes*, March 21, 2012, https://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/?sh=377debb81f74; Charlie Osborne, "NSA Purchased Zero-Day Exploits from French Security Firm Vupen," ZDNET/Tech, September 18, 2013, https://www.zdnet.com/article/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen/.

180 "VUPEN SECURITY (Company Profile): Fermée définitivement [Closed permanently], Chiffre d'affaires [key figures]," Societe (Paris, France), accessed July 3, 2024, https://www.societe.com/societe/vupen-security-478502123.html#chiffrecle.

181 "ZERODIUM LLC (Company Profile)," OpenCorporates, accessed July 3, 2024. https://opencorporates.com/companies/us_de/5811248.

182 Lily Hay Newman, "Zerodium Zero Day iOS Bounty Is Now $1.5 Million," *Wired*, September 29, 2016, https://www.wired.com/2016/09/top-shelf-iphone-hack-now-goes-1-5-million/.

183 Gintaras Radauskas, "OpZero Raises Stakes in Zero-Day Exploit Market," *Cybernews*, November 15, 2023 [update], https://cybernews.com/news/opzero-zero-day-exploit-market-pricing-russia/.

184 "Zerodium (Company Profile)," Info Security Index (Infosecindex), accessed July 3, 2024. https://infosecindex.com/companies/zerodium/.

VENDORS

Aglaya Scientific Aerospace Technology Systems Private Limited

Aglaya Scientific Aerospace Technology Systems Private Limited (Aglaya) was founded in 2014 in India by Ankur Srivastava. In addition to spyware services, Aglaya markets itself as a zero-day seller and a censorship-as-a-service company specializing in online trolling and disinformation.[185] Offering to run its buyer's spyware operations for 2,500 euros per day and 600 euros for disinformation campaigns, Agalya positions itself in an interesting space in this market as it sells to non-government entities.[186]

The financial structure of the company is also entirely based in India, with holding companies becoming inactive in 2021, alongside the vendor itself. Aglaya was included in this research report to highlight the market for spyware outside of corporate-to-government sales, as well as the wide range of product types offered by full-service vendors, which can include not only the spyware product itself but command and control package offerings.

Cognyte Software Ltd.

Cognyte Software Ltd. was established as an independent company in 2020, registered in Israel, after the US-based Verint Systems Inc. separated its customer engagement business from its cyber intelligence business due to shareholder pressure. As a result of the separation, Cognyte Software Ltd. focuses on the "security analytics software market."[187] Its CEO is Elad Sharon and has subsidiaries in India, Brazil, Bulgaria, Canada, Delaware USA, Mexico, the United Kingdom, Israel, Taiwan, Thailand, Germany, Cyprus, the Netherlands, and Romania. Cognyte is a public company that trades its shares on the NASDAQ, with Visa Equity Partners as its largest institutional shareholder.[188]

Cognyte Software Ltd., however, has a history dating back to 1994 when Verint Systems Inc. was incorporated as Interactive Information Systems Corporation in the United States. The firm developed AudioDisk, a digital surveillance product intended to be used by police and intelligence agencies to record and store wiretap material.[189] Two years later, the company changed its name to Comverse Information Systems Corporation, which later merged with Comverse InfoMedia Systems to create Comverse Infosys.[190] The US Department of Defense is known to be a customer of Comverse Infosys' AudioDisk product.[191] After the 9/11 attacks, Comverse Infosys changed its name to Verint Systems Inc. and launched its Initial Public Offer (IPO).[192] In 2013, Verint Systems Inc. was separated from other businesses of Comverse Technology and made a standalone company with Dan Bodner as its CEO.[193] This is the company that eventually became Cognyte Software Ltd.

The company and its subsidiaries have been in controversies since its inception. In 2001, Fox News reported that AudioDisk used by the US government may have been vulnerable, as these systems allegedly had a back door through which the wiretaps could be intercepted by unauthorized parties.[194]

In 2006, it was delisted from the NASDAQ due to allegations of being a part of an options backdating scandal.[195] In its 2021 Threat Report on the Surveillance-for-Hire Industry[196], Meta announced that it removed around one hundred Facebook and Instagram accounts linked to Cognyte Software Ltd. The report claimed that Cognyte Software Ltd. "sells access to its platform which enables managing fake accounts across social media platforms to social-engineer people and collect data."[197] Most recently in 2022, the Norwegian Government Pension Fund Global (GPFG) was recommended by the

185 Franceschi-Bicchierai, Lorenzo, "This Leaked Catalog Offers 'Weaponized Information' That Can Flood the Web," Vice (blog), September 2, 2016, https://www.vice.com/en/article/d7ywvx/leaked-catalog-weaponized-information-twitter-aglaya.

186 Thomas Brewster, "Meet The 'Cowboys of Creepware'– Selling Government-Grade Surveillance to Spy on Your Spouse," *Forbes*, March 14, 2017, https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware/?sh=71933002455c.

187 "Amendment No. 1 to Form 20-F: Cognyte Software Ltd.," January 13, 2021, https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351d20fr12ba.htm.

188 "Cognyte Software Ltd. (CGNT) DCF Valuation," dcf.fm, accessed July 31, 2024, https://dcf.fm/products/cgnt.

189 "Verint Systems Inc.," International Directory of Company Histories, Encyclopedia.com, accessed July 31, 2024, https://www.encyclopedia.com/books/politics-and-business-magazines/verint-systems-inc.

190 "Verint Systems Inc."

191 "Verint Systems Inc."

192 "Verint Systems Inc."

193 "Comverse Technology," Wikipedia, accessed July 31, 2024, https://en.wikipedia.org/wiki/Comverse_Technology.

194 *Censored Israeli Software Spying On US Am Docs Comverse Infosys Carl Cameron Dec 2001*, 2013, http://archive.org/details/CensoredIsraeliSoftwareSpyingOnUSAmDocsComverseInfosysCarlCameronDec2001.

195 "Former Comverse CEO Agrees to $53 Million Settlement of Options Backdating Charges (Press Release No. 2010-232; November 23, 2010," accessed July 31, 2024, https://www.sec.gov/news/press/2010/2010-232.htm.

196 Dvilyanski, Agranovich, and Gleicher, "Threat Report on the Surveillance-for-Hire Industry."

197 Dvilyanski, Agranovich, and Gleicher, "Threat Report on the Surveillance-for-Hire Industry."

country's Council on Ethics to divest from Cognyte Software Ltd. due to the "unacceptable risk that the company is contributing to serious human rights abuses."[198]

Cyber Root Risk Advisory Private Limited

CyberRoot Risk Advisory Private Limited (CyberRoot) was founded in India in 2013 by Vijay Singh Bisht, Chiranshu Ahuja, and Vibhor Sharma.[199] In 2013, CyberRoot entered a relationship of "information sharing" with Appin Security Group and BellTroX Infotech Services Private Ltd., both classified as spyware vendors within this dataset. The nature of this information sharing or when it ended is unclear.[200] CyberRoot, unlike its other Indian vendor counterparties, has a holding company within the United Kingdom named CyberRoot Limited.[201]

DataForense s.r.l.

Founded in Italy by Annunziata Cirilloin in 2013,[202] Dataforense s.r.l. is known for its spyware Aretmide/Spyrtacus project. This system allows users to extract data from phones running Android or iOS.[203] The company was in liquidation as of 2024 according to the Italian business registry.[204] There was little available information about this particular vendor, but it was included in this report and dataset to show the subcluster of vendors emerging in Italy.

DSIRF GmbH

Founded in 2016 in Austria by Stefan Gesselbauer, DSIRF GmbH is known for its spyware SubZero.[205] The company has one known subsidiary, MLS Machine Learning Solutions GmbH, which specializes in the development and implementation of machine learning models.[206] In 2023, the vendor entered liquidation proceedings within the Vienna Court of Commerce.[207] It is believed its subsidiary, MLS Machine Learning Solutions, is absorbing the business of DSIRF, and that DSIRF's lead investor, DSR Decision Supporting Information Forensic, will continue to support the company.[208]

Gamma Group International SAL

First registered in Germany in 2008, Gamma International GmbH, later renamed to FinFisher Labs GmbH in 2012, is the vendor of FinSpy spyware.[209] FinFisher Labs GmbH, in collaboration with their supplier, Elaman GmbH, distributed FinSpy to a variety of different government clientele, including entities in Singapore, South Africa, and Turkey, but remained an exclusively German-domiciled vendor.[210] In 2022, FinFisher Labs GmbH shut down operations in Germany after legal prosecution.[211] Gamma Group's holding companies are almost entirely in the United Kingdom, British Virgin Islands, and Cyprus and are associated with a single family. These holding companies might be used to filter investment from this family to Gamma Group. Thus, while Gamma Group is no longer operational within Germany, its financial structure and potentially its investment base are operational.

InvaSys a.s.

In 2017, Kyrre Sletsjøe founded InvaSys a.s. in Czechia.[212] The company specializes in mobile phone interception and qualifies as both a funder and a supplier due to its

198 "Recommendation to Exclude Cognyte Software › from Investment by the Norwegian Government Pension Fund Global (GPFG)" (Council on Ethics, The Government Pension Fund Global, June 17, 2022), https://files.nettsteder.regjeringen.no/wpuploads01/sites/275/2022/12/Rec-Cognyte-ENG.pdf.

199 Satter and Bing, "How Mercenary Hackers Sway Litigation Battles."

200 Satter and Bing, "How Mercenary Hackers Sway Litigation Battles."

201 "Cyber Root Limited (Company Profile)," Gov.UK (UK Department for Business & Trade: Companies House), accessed July 11, 2024, https://find-and-update.company-information.service.gov.uk/company/14414734.

202 "Business registers-search for a company in the EU," *European-Justice,* Accessed July 11, 2024, https://e-justice.europa.eu/489/EN/business_registers__search_for_a_company_in_the_eu.

203 "SIO follows Europe cyber offensive consolidation trend with Asingit acquisition." *Intelligence Online,* March 3, 2022, https://www.intelligenceonline.com/surveillance--interception/2022/03/03/sio-follows-european-cyber-offensive-consolidation-trend-with-asingit-acquisition,109737657-art.

204 "Business registers-search for a company in the EU," *European-Justice,* Accessed July 11, 2024, https://e-justice.europa.eu/489/EN/business_registers__search_for_a_company_in_the_eu.

205 Andre Meister, "We reval the state trojan "SubZero" from Austria," *Netzpolitik,* December 17, 2021, https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.

206 "MLS Machine Learning Solutions," *North Data,* Accessed July 30, 2024, "https://www.northdata.com/MLS+Machine+Learning+Solutions+GmbH,+Wien/521402v.

207 "Targeted for Russian ties, cyber intelligence firm DSIRF shuts up shop," *Intelligence Online,* August 28, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/08/28/targeted-for-russian-ties-cyber-intelligence-firm-dsirf-shuts-up-shop,110036360-art

208 "TTargeted for Russian Ties, Cyber Intelligence Firm DSIRF Shuts up Shop." *Intelligence Online,* August 28, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/08/28/targeted-for-russian-ties-cyber-intelligence-firm-dsirf-shuts-up-shop,110036360-art.

209 "Company Register," accessed July 3, 2024, https://www.unternehmensregister.de/ureg/result.html;jsessionid=635E5C635A2A17FAAE4DB7AB9D7547DB.web01-1.; Feldstein and Kot, "Why Does the Global Spyware Industry Continue to Thrive?"

210 Feldstein and Kot, "Why Does the Global Spyware Industry Continue to Thrive?"

211 "Finfisher Ceases Business Operations Following Criminal Complaint against Illegal Export of Surveillance Software," Business & Human Rights Resource Centre, March 28, 2022, https://www.business-humanrights.org/en/latest-news/finfisher-ceases-business-operations-following-criminal-complaint-against-illegal-export-of-surveillance-software/; Andre Meister, "State Trojan Manufacturer FinFisher 'Is Closed and Will Remain So,'" Netzpolitik.org, March 28, 2022, https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/.

212 Veřejný Rejstřík a Sbírka Listin – InvaSys a.s." [Public Register and Collection of Deeds – InvaSys a.s.], eJustice (Ministry of Justice of the Czech Republic), accessed July 3, 2024, https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=47757423&subjektId=967334&spis=1068597.

production of spyware tools and its sales of zero-day vulnerabilities.[213] Notably, the company's Kelpie program provides backdoor access to Android and iPhone devices and encrypted messaging applications.[214] The company operates out of two offices in Czechia: one in Brno and another in Prague. Founder and CEO Kyrre Sletsjøe also owns and runs Defense System Property Protection, a physical security firm, and YX Systems. Some InVasys employees previously worked at Sletsjøe's prior company CEPIA Technologies.[215] From March to August of 2017 Thomas Vestyby Jensen was listed as the sole owner of InVasys Technologies; however, as of 2022, Kyrre Sletsjøe has a ninety-one percent ownership stake in InvaSys. At present the company has not faced any challenges to its operations in Czechia.[216]

Leo Impact Security Services

Founded in 2009 by Manish Kumar, Leo Impact Security Services is listed as a vendor in the dataset.[217] There has been some reporting that this vendor is a direct competitor of Aglaya, another spyware vendor profiled for this report, as they offer similar spyware products.[218] It has one branch based in Czechia named Leo Impact Security s.r.o. that has been operational since 2010.[219]

Mollitiam Industries

Mollitiam is a Spanish vendor founded in 2018 by In-Nova and the cybersecurity firm StackOverflow Ltd. It is headed by Santiago Molins Riera, who is the former head of technology of In-Nova.[220] Mollitiam is known to develop payloads that can intercept communications and steal cloud-hosted data from infected devices and deploy spyware on Microsoft, Apple, and Google mobile devices and operating systems. It is known for its interception tools Invisible Man and Night Crawler, which are capable of remotely accessing files and location data and covertly turning on a device's camera and microphone.[221]

Mollitiam has provided services to Spain's National Intelligence Centre (CNI) and Mando Conjunto de Ciberdefensa (MCCD), the country's joint cyberspace command.[222] It receives funding from the Centre for the Development of Industrial Technology (CDTI) which is a public corporation under the Spanish Ministry of Economy and Competitiveness.[223] The European Union's Regional Development Fund provided financial support to Mollitiam between 2019 and 2021 for a project worth €650,000 to build a platform to provide new ways to automatically generate intelligence from data extracted from social media platforms and the dark web.[224] Apart from these government funds, venture capital firms like EASO Ventures, Sabadell Venture Capital, and Torsa Capital have investments in this Spanish firm.[225]

Movia S.p.A.

Movia S.p.A. is an Italian spyware vendor founded in 2003 by Luca Spina. It is known to sponsor ISS World, a global surveillance technology trade.[226] The company's spyware product is called Spider and is used by prosecution offices in Italy. In 2022, the company established a subsidiary called Bioss, and Spina launched another company called Vision s.r.l.[227] Movia's largest investor is known to be Sistema Investimenti.[228] Movia was exposed by the Italian

213 "Invasys: Solutions," Invasys a.s., accessed July 3, 2024, https://www.invasys.com/solutions/.

214 Omer Benjakob, "At Defense and Arms Expo, Israeli Cyber Is Out, but Surveillance Tech in," Haaretz, December 8, 2023, https://www.haaretz.com/israel-news/security-aviation/2023-12-08/ty-article/.premium/at-defense-and-arms-expo-israeli-cyber-is-out-but-surveillance-tech-in/0000018c-49da-db23-ad9f-69da26e10000.

215 "Veřejný Rejstřík a Sbírka Listin – InvaSys a.s." [Public Register and Collection of Deeds – InvaSys a.s.].

216 "Veřejný Rejstřík a Sbírka Listin – InvaSys a.s." [Public Register and Collection of Deeds – InvaSys a.s.].

217 "Leo Impact Security Services Private Limited (Company Profile)," Zaubacorp (Zauba Technologies), July 9, 2024, https://www.zaubacorp.com/company/LEO-IMPACT-SECURITY-SERVICES-PRIVATE-LIMITED/U72900RJ2009PTC028837.

218 "Cyber offensive firm Leo Impact competing with Aglaya for greater share in surveillance domain," Medium (blog), June 22, 2023, https://mahdiabbastech.medium.com/cyber-offensive-firm-leo-impact-competing-with-aglaya-for-greater-share-in-surveillance-domain-965187dff2d.

219 "Leo Impact Security s.r.o.", Ministry of Justice of the Czech Republic, Accessed July 11, 2024, https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=389677&typ=UPLNY.

220 "The Tech Times: Mollitiam Gets New CEO, Paolo Stagno Joins Crowdfense, Whooster Assists US Secret Service," Intelligence Online, January 11, 2024, https://www.intelligenceonline.com/surveillance--interception/2024/01/11/mollitiam-gets-new-ceo-paolo-stagno-joins-crowdfense-whooster-assists-us-secret-service,110136850-art.

221 Bruce Schneier, "Mollitiam Industries Is the Newest Cyberweapons Arms Manufacturer," Schneier on Security (author blog), June 23, 2021, https://www.schneier.com/blog/archives/2021/06/mollitiam-industries-is-the-newest-cyberweapons-arms-manufacturer.html.

222 "Europe, Israel: Excem, Israeli Cyber's Bridgehead in Spain," Intelligence Online, May 20, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/05/20/excem-israeli-cyber-s-bridgehead-in-spain,109667518-art.

223 "Centre for the Development of Industrial Technology (Company Profile)," Crunchbase, accessed July 3, 2024, https://www.crunchbase.com/organization/centre-for-the-development-of-industrial-technology-cdti.

224 "ERDF Pluri-Regional Operational Programmes," DGFE (Spain Directorate General for European Funds), accessed July 3, 2024. https://www.fondoseuropeos.hacienda.gob.es/sitios/dgfc/en-GB/IoFEDER1420/popIFEDER/Paginas/inicio.aspx.

225 "ERDF Pluri-Regional Operational Programmes"; "Mollitiam Industries (Company Profile: Valuation and Funding)," PitchBook," accessed July 3, 2024, https://pitchbook.com/profiles/company/462012-40.

226 Patrick Howell O'Neill, "ISS World: The Traveling Spyware Roadshow for Dictatorships and Democracies," CyberScoop, June 20, 2017, https://www.cyberscoop.com/iss-world-wiretappers-ball-nso-group-ahmed-mansoor/. ; "Italy: Italian Cyber Intelligence Specialist Movia Goes Global," Intelligence Online, November 8, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/11/08/italian-cyber-intelligence-specialist-movia-goes-global,110085487-art.

227 "Italian Cyber Intelligence Specialist Movia Goes Global."

228 "Italian Cyber Intelligence Specialist Movia Goes Global."

anti-terrorist and anti-mafia investigative directorate called Direzione Nazionale Antimafia e Antiterrorismo (DNAA).[229]

negg Group s.r.l.

In 2013, Francesco Taccone co-founded negg Group s.r.l. in Italy.[230] By 2017, Kaspersky Lab published a report detailing the invasive capabilities of Skygofree, a spyware tool it attributes to negg Group.[231] Skygofree ties many of its exploitive services, including audio recordings and photo captures on target devices, to the device location.[232] For example, Skygofree allows attackers to turn on audio recording capabilities when they deem that a device has entered a sensitive location such as a meeting or product development site.[233] Furthermore, the spyware tool forces infected devices to connect to attacker-controlled WiFi networks, offering attackers the ability to collect and analyze WiFi traffic. Finally, this spyware tool exploits vulnerabilities within a device's accessibility services to allow attackers to read encrypted WhatsApp messages. As of 2024, Meta observed the negg Group accounts testing exploit delivery via Facebook and Instagram and consequently removed its accounts from these platforms.[234] The company maintains three offices registered in Italy: two in Rome and one in Reggio Calabria.[235] Between 2020 and 2022 negg International operated in the Netherlands under the ownership of companies with ties to the negg Group co-founder.[236] However, the business relationship between negg Group and negg International remains unknown at this time. In 2014, the Italian Ministry of Economic Development awarded negg Group a digitalization voucher worth 9,872 euros.[237] At the time, such vouchers were intended to support the digital transformations of Italian companies. At present, the negg Group website states that the company "actively seeks" investors.[238]

Positive Technologies AO

Founded by Yuri Maksimov and Dmitry Maximo in 2002, Positive Technologies AO is a Russian company that was added to the list of entities sanctioned by the US Office of Foreign Assets Control (OFAC) in 2021 on account of its role in the organization of the Positive Hack Days cybersecurity conference. The conference is said to be used by the Russian Federal Security Service (FSB) for recruitment, according to the US Treasury Department. The Bureau of Industry and Security (BIS) of the US Department of Commerce also accused Positive Technologies AO of distributing exploits and added it to the Entity List for malicious cyber activities.[239] The US Department of State announced the vendor was listed based on a determination that it "misuse[s] and traffic[s] cyber tools that are used to gain unauthorized access to information systems in ways that are contrary to the national security or foreign policy of the United States, threatening the privacy and security of individuals and organizations worldwide."[240] Positive Technologies AO has a corporate presence in at least six different countries.

According to Intelligence Online, Positive Technologies operates two websites—one for the Russian market and another for the international market. On its website for the international market, the vendor lists Lukoil, Vimpelcom, Sberbank, the South Korean companies Hanwha and Samsung, France's Societe Generale bank, and the French cybersecurity agency, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), as its clients.[241]

229 Marco Bova, "Una ditta di intercettazioni nelle indagini sul sistema Montante" [A wiretapping firm in the investigations on the Montante system], *L'Espresso,* August 9, 2022, https://lespresso.it/c/attualita/2022/8/9/una-ditta-di-intercettazioni-nelle-indagini-sul-sistema-montante/12796.

230 "Negg Group© (Company Profile)," Crunchbase, accessed July 3, 2024, https://www.crunchbase.com/organization/negg.

231 Nikita Buchka and Alexey Firsh, "Skygofree: Following in the Footsteps of HackingTeam," Securelist, January 16, 2018, https://securelist.com/skygofree-following-in-the-footsteps-of-hackingteam/83603/.

232 Buchka and Firsh, "Skygofree: Following in the Footsteps of HackingTeam."

233 Buchka and Firsh, "Skygofree: Following in the Footsteps of HackingTeam."

234 Ben Nimmo et al., "Adversarial Threat Report: Countering the Surveillance-for-Hire Industry & Influence Operations," 2023, https://about.fb.com/wp-content/uploads/2023/06/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf.

235 "Negg® Group | Find Us." n.d. Accessed July 3, 2024. https://www.negg.group/offices.

236 "Negg International B.V. (Company Profile)," OpenCorporates," accessed July 3, 2024, https://opencorporates.com/companies/nl/80409644; "Italy: Italian Intelligence Provider Negg Makes Entrance at ISS World Exhibition," Intelligence Online, September 1, 2022, https://www.intelligenceonline.com/surveillance--interception/2022/09/01/italian-intelligence-provider-negg-makes-entrance-at-iss-world-exhibition,109808500-art.

237 "Voucher Digitalizzazione, Elenco Cumulativo Dei Soggetti Beneficiari – Regione Calabria" [Digitization Voucher, Cumulative list of beneficiaries – Calabria region], MIMIT (Italy: Ministry of Enterprises and Made in Italy, formerly the Ministry of Economic Development), September 9, 2014, https://www.mimit.gov.it/images/stories/normativa/Allegato_A_-_Calabria.pdf; "Digitization Vouchers 2021: We Help You Get Them," Digitalics Innovation, accessed July 3, 2024, https://digitalicsinnovation.com/en/voucher-digitalizzazione-2021-innovazione-aziendale/.

238 "Negg® Group – Investors," accessed July 3, 2024. https://www.negg.group/investors/overview.

239 "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," U.S. Department of Commerce, Accessed July 28, 2024, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

240 "CHINA/SINGAPORE/UNITED STATES : Blacklisted by the US, Zero Day Distributor COSEINC Works on for China's Pwnzen - 08/11/2021." 2024. Intelligence Online. July 3, 2024. https://www.intelligenceonline.com/surveillance--interception/2021/11/08/blacklisted-by-the-us-zero-day-distributor-coseinc-works-on-for-china-s-pwnzen,109703349-art.; "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities - United States Department of State." n.d. Accessed July 3, 2024. https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/.

241 "Spotlight / China, Russia: Huawei Hired Top Researchers from Russia's US-Sanctioned NeoBit," Intelligence Online, June 18, 2021, https://www.intelligenceonline.com/corporate-intelligence/2021/06/18/huawei-hired-top-researchers-from-russia-s-us-sanctioned-neobit,109674074-eve.

RCS Labs

Founded in 1992 in Italy, RCS Labs (RCS ETM Sicurezza S.p.A) operates as both an original producer as well as an intermediary seller of spyware.[242] As early as 2012, RCS facilitated the sale of Hacking Team srl products and services, including Hacking Team srl's Remote Control System (RCS), to government agencies in Bangladesh, Pakistan, and Turkmenistan.[243] In 2022, security researchers at Lookout determined RCS Lab S.p.A created and sold the Hermit spyware.[244]

The RCS Group (formerly Aurora Group) owns RCS Labs. In March 2022, another Italian firm that sells spyware amongst other products, Cy4Gate, acquired Aurora Group, including its seven subsidiary companies: RCS ETM Sicurezza S.p.A., RCS LAB GMBH, Tykelab, Azienda Informatica Italiana, Servizi Tattici Informativi Legali, Dars Telecom SL, and Aurora France S.A.S.[245] Cy4Gate is one of Italy's largest technology companies, is publicly traded, and its primary investors are Elettronica Group and Expert System. According to Cy4Gate's 2023 financial reporting, RCS Labs remains the most profitable company in the Aurora Group.[246]

Variston Information Technology

Variston Information Technology (Variston) was founded in 2018 by Ralf Wegener and Ramanan Jayaraman and is headquartered in Barcelona, Spain.[247] Variston is known to develop data collection tools for law enforcement and security solutions in the areas of supervisory control and data acquisition (SCADA) and the Internet of Things (IoT).[248] Shortly after its incorporation in 2018, Variston IT acquired Truel IT,[249] an Italian zero-day vulnerabilities research company. This acquisition helped Variston onboard new researchers and capabilities, including developing its spyware Heliconia.[250] According to reporting from Intelligence Online in May 2024, Variston Information Technology is now effectively defunct.[251]

242 Cy4Gate S.p.A., "Press Reports," press note, June 24, 2022, https://www.cy4gate.com/assets/Uploads/CS-CY4gate-Nota-stampa-RCS.pdf.

243 "Re: PAF and PN," WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024, https://wikileaks.org/hackingteam/emails/emailid/599145; "RE: Proposal GD6 (via CNC)," WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024, https://wikileaks.org/hackingteam/emails/emailid/16869; "Re: HT & RCS cooperation," WikiLeaks (Hacking Team srl Archive), accessed July 3, 2024. https://wikileaks.org/hackingteam/emails/emailid/567762.

244 "Lookout Uncovers Hermit Spyware Deployed in Kazakhstan," Lookout Threat Intelligence, June 16, 2022, https://www.lookout.com/threat-intelligence/article/hermit-spyware-discovery.

245 "The Cy4Gate Group – Corporate Data of the Parent Company," Cy4Gate S.p.A., n.d., https://www.cy4gate.com/assets/Uploads/Consolidated-Financial-Statement-CY4Gate-Group-30.6.2022-ENG-Courtesy-copy.pdf.

246 "Cy4Gate S.P.A. Interim Financial Report," Cy4Gate S.p.A., June 30, 2023, https://www.cy4gate.com/assets/Uploads/Interim-Financial-Report-as-at-30-June-2023.pdf.

247 Clement Lecigne and Benolt Sevens, "New Details on Commercial Spyware Vendor Variston," Google Threat Analysis Group, November 30, 2022, https://blog.google/threat-analysis-group/new-details-on-commercial-spyware-vendor-variston/.

248 "Europe: German Ralf Wegener Builds Small Cyber-Intelligence Empire in Cyprus and Beyond," Intelligence Online, October 22, 2021, https://www.intelligenceonline.com/surveillance--interception/2021/10/22/german-ralf-wegener-builds-small-cyber-intelligence-empire-in-cyprus-and-beyond,109700415-gra.

249 "Europe: Commercial Cyber Bosses Ralf Wegener and Ramanan Jayaraman Operate Singapore-Based Nanostrea," Intelligence Online, March 3, 2023, https://www.intelligenceonline.com/surveillance--interception/2023/03/03/commercial-cyber-bosses-ralf-wegener-and-ramanan-jayaraman-operate-singapore-based-nanostrea,109919867-art.

250 Lecigne and Sevens, "New Details on Commercial Spyware Vendor Variston."

251 "Ex-Variston zero day experts regroup at Paradigm Shift," *Intelligence Online,* May 15, 2024, https://www.intelligenceonline.com/surveillance--interception/2024/05/15/ex-variston-zero-day-experts-regroup-at-paradigm-shift,110226089-art. This section has been updated to clarify the description of recent reporting on Variston Information Technology.

Appendix B — Markets Map: Country list (42)

Australia	Hungary	Qatar
Austria	India	Romania
Bahrain	Ireland	Russia
Bangladesh	Israel	Singapore
Belgium	Italy	South Africa
Brazil	Lebanon	South Korea
British Virgin Islands	Liechtenstein	Spain
Bulgaria	Luxembourg	Switzerland
Canada	Malta	Taiwan
Cyprus	Mexico	Tunisia
Czechia	Netherlands	Turkey
France	North Macedonia	United Arab Emirates
Germany	Norway	United Kingdom
Greece	Oman	United States

Appendix C — Markets Map: Vendor List (49)

Aglaya Scientific Aerospace Technology Systems Private Limited

Appin Security Group > Approachinfinate Computer and Security Consultancy Grp.
- » Adaptive Control Security Global Corporate

BellTroX Infotech Services Private Ltd

Candiru Ltd > DF Associates > Grindavik Solutions Ltd./ Greenwick Solutions > Taveta Ltd./Tabatha Ltd > Saito Tech Ltd.

CyberRoot Risk Advisory Private Limited > CyberRoot Software Solutions LTD

Cytrox AD
- » Intellexa S.A.

Dataflow Security s.r.l.

DataForense s.r.l

DSIRF GmbH

Equus Technologies > MerlinX Ltd.

Gamma Group International SAL
- » Gamma International GmbH > FinFisher Labs Gmbh

Hacking Team srl (Italy) > Memento Labs srl
- » Hacking Team srl (United States)
- » Grey Heron (United Kingdom)
- » Grey Heron (Italy)

Interionet Systems Ltd.

InvaSys a.s.

Leo Impact Security Service PVT Ltd.
- » Leo Impact Security s.r.o.

Mollitiam Industries

Movia SPA

Negg Group S.R.L
- » Negg International

NSO Group
- » L.E.G.D Technologies > Q Cyber Technologies
- » Westbridge Technologies
- » Osy Technologies SARL
- » Q Cyber Technologies SARL

Paragon Solutions

Positive Technologies AO (Russia)[252]
- » Positive Technologies Global Holding Ltd. (United Kingdom)
- » Positive Technologies Global Solutions Ltd. (United Kingdom)
- » Positive Technologies S.R.L (Romania)
- » Positive Technologies S.R.L. (Italy)
- » Positive Technologies Inc. (United States)
- » Positive Technologies Czech s.r.o. (Czech Republic)
- » Positive Technologies Holding AG (Switzerland)

Quadream Inc.

RCS ETM Sicurezza S.p.A.
- » RCS MEA DMCC

Variston IT

Verint Systems Inc.
- » Verint Systems Ltd.
- » Cognyte Software Ltd. (Israel)

252 Sourcing from Positive Technologies website indicates there are branches of the company in South Korea and Tunisia. However, the authors were unable to find corporate registrations of these companies in these jurisdictions and thus they are not included in the dataset.

ABOUT THE AUTHORS

Jen Roberts is an Assistant Director with the Atlantic Council's Cyber Statecraft Initiative. She primarily works on CSI's Proliferation of Offensive Cyber Capabilities and Combating Cybercrime work. Jen also helps support the Cyber 9/12 Strategy Challenge and is passionate about how the United States with its allies and partners, especially in the Indo-Pacific, can cooperate in the cyber domain. Jen holds an MA in International Relations and Economics from Johns Hopkins University's School of Advanced International Studies (SAIS) where she concentrated in Strategic Studies. She also attained her BA in International Studies from American University's School of International Service.

Trey Herr is assistant professor of Global Security and Policy at American University's School of International Service and Senior Director of the Atlantic Council's Cyber Statecraft Initiative. At the Council, the CSI team works at the intersection of cybersecurity and geopolitics across conflict, cloud computing, supply chain policy, and more. At American, Trey's work focuses on complex interactions between states and non-state groups, especially firms, in cyberspace. Previously, he was a senior security strategist with Microsoft handling cybersecurity policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Nitansha Bansal is an assistant director with the Cyber Statecraft Initiative (CSI), part of the the Atlantic Council Tech Programs. In this role, her research focuses on the proliferation of offensive cyber capabilities, including spyware and its policy implications for human rights and national security, and open source software security. She also supports the capacity building efforts of CSI, and runs the Congressional Cyber and Digital Policy Program.

Prior to joining the Council, Nitansha worked with government and think tanks in India on technology policy. She holds a masters in public administration from Columbia University's School of International and Public Affairs where she concentrated on cybersecurity and business risk, social media policy, and data analysis.

Nancy Messieh is Deputy Director for Visual Communications with the Atlantic Council's Cyber Statecraft Initiative, where she focuses on visual storytelling and data visualization.

Emma Taylor is a Research Assistant with the School of International Service and a highly interdisciplinary professional pursuing an M.S. in Computer Science and Cybersecurity with previous experience in the technology industry.

Jean Le Roux conducted this research as a research associate for the Sub-Saharan Africa region at the Atlantic Council's Digital Forensic Research Lab (DFRLab). He is now a senior investigator at Graphika.

Sopo Gelava is a research associate for the Caucasus with the Atlantic Council's Digital Forensic Research Lab. Prior to the DFRLab, she served as media literacy programs director at Media Development Foundation, leading Georgian think-tank countering disinformation and information operations.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
Dario Deste
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of April 24, 2024

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.
1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org