LONDON POLITICA

REPORT

Overlooked Risks – Emergent Technologies

Growing Global Market and Demand for Malware-as-a-Service

April 2024

Ella Startt, Kathryn Hockman, Bosco Hung, Christopher Healey, Angus Robins & Anonymised London Politica Analyst

REPORT

Overlooked Risks – Emergent Technologies

Growing Global Market and Demand for Malware-as-a-Service

April 2024

Ella Startt, Kathryn Hockman, Bosco Hung, Christopher Healey, Angus Robins, & Anonymised London Politica Analyst.

London Politica

About us

London Politica

London Politica is the world's largest political risk advisory for social impact. We support our diverse range of clients with bespoke analysis and actionable intelligence to empower them to navigate the increasingly volatile political environment.

London Politica was set up to democratise political risk. We aim to provide political risk analysis and forecasting to those organisations, NGOs, and companies who need it most, operating in some of the globe's most unstable regions, but who do not necessarily have the capacity traditionally to employ such counsel.

By bridging this gap, London Politica aims to be a force for good, in an industry otherwise short of young perspectives. Our talented team of analysts offer fresh insight into local, regional, and global trends.

Emergent Technologies Programme

Emergent Technologies as a term is used to denote either new or a continued development of an existing technology. Artificial Intelligence (AI), quantum computing, autonomous systems, and synthetic biology are some of the trends which have a significant impact on society. However, geopolitics interacting with these technologies can introduce significant risks to individuals, businesses, governments, policymakers and NGOs.

The Emergent Technologies programme works at the intersection of these technologies and political risk with the aim to provide research and analysis to navigate political risks and drive growth. The recognition of these key technology trends, with the backdrop of London Politica's broader expertise in geopolitical risk allows for the provision of comprehensive and integrated actionable insights.

Authors

Ella Startt

Ella Startt is the Assistant Director of the Emergent Technologies Programme at London Politica. Her interests revolve around the intersection between technology and geopolitics, primarily in Europe and East, South or Central Asia. She also works as a Contributor for Oxford Analytica in political risk for South Korea and in EU Advocacy at Foundation the London Story, an NGO which focuses on disinformation, hate speech and tech harms in India. Ella has previously held research positions at LSE and at the U.S. Committee for Human Rights in North Korea. She did a BA in War Studies and Philosophy from King's College London, and is studying an MSc in Cybersecurity Governance at Leiden University.

Kathryn Hockman

Kathryn Hockman is a Programme Analyst with London Politica's Emergent Technologies Programme. Her research interests centre around the intersection between policy and responsible technology development, with a focus on how governments understand and interact with emerging technologies. She currently serves as an Affiliate Champion for the Women in Cybersecurity UK Affiliate and is passionate about improving opportunities for women in technology. She holds a MA in Conflict, Security and Development from King's College London.

Bosco Hung

Bosco Hung is a Consultant at London Politica. He is a BSc in Politics and International Relations student at London School of Economics. He has held research positions at numerous academic associations and geopolitical consultancies, such as the International Team for the Study of Security Verona, the Nicholas Spykman International Center for Geopolitical Analysis, and the Global Studies Institute in Hong Kong. He has researched Chinese politics and emerging technology and has spoken on France 24 and Al Jazeera. He has written for Connections: The Quarterly Journal, The Journal of Conflict, Intelligence, and Warfare, The National Interest, UDN, Initium Media, and other peer-reviewed publications and newspapers. His research was presented in the UK Parliament, the Oxford Hong Kong Forum, and other professional settings.

Christopher Healey

Christopher Healey is the Assistant Programme Director of the Europe Programme at London Politica, where he researches transatlantic security issues and European and American politics and supports business development efforts. He previously worked in Washington, DC, at the American Enterprise Institute and the Center for Strategic & International Studies in outreach and communications roles, respectively. He also interned with the Critical Threats Project at the American Enterprise Institute and a Deloitte subsidiary in Paris. Mr. Healey is an alum of Kenyon College in Ohio and is from Boston, Massachusetts, and Evanston, Illinois.

Angus Robins

Angus Robins, a seasoned professional with a Master's degree in Politics of the Middle East, seamlessly transitioned into the realm of technology, cyber, and data. His diverse background and keen interest in the industry led him to excel in high-level technology recruitment, where he identified and nurtured top talent. In coming months, Angus will be embarking on a technology-focused role in the Civil Service.

Anonymised London Politica Analyst

This author has chosen to retain anonymity

Contents

Executive Summary

- The global market for malware-as-a-service (particularly spyware-as-a-service products) continues to expand and has sweeping implications for the health of democracies and civil society. While branded as an anti-terrorist and anti-crime tool, spyware is increasingly being leveraged by both authoritarian and democratic regimes as a technique of digital repression to suppress and spy on domestic opposition figures and movements. The targeting of civil society actors poses a significant risk to free expression in illiberal and democratic countries alike.

- Private sector companies are producing increasingly powerful spyware technology that can infiltrate a device, some without action from the device owner (such as clicking on a phishing link). Once installed, a spyware has virtually unimpeded access to the device's private information, and can even manipulate its functions, such as a mobile phone's camera and microphone. At least 18 companies selling spyware-as-a-service products have contracts with 74 different governments, and the industry is estimated to be valued at roughly USD 12 billion.

- The most well-known of these companies is the Israeli NSO Group, which produces Pegasus, a highly effective spyware technology that can infiltrate iOS and Android devices nearly undetected. Yet, NSO is not the largest seller, with Finfisher recording a record number of 34 government contracts.

- To combat the dangers posed by spyware, comprehensive legislation to reduce the development and sale of spyware products is needed from national governments and supranational entities such as the European Union. Moreover, there is a greater need for research from private and third-sector organizations about the impact of spyware on civic health and the security of technological devices. Private sector companies, as the producer of devices, have an especially important role in strengthening the defence of their products against spyware intrusion.

Section 1

How the Spyware Market extends beyond Pegasus

Spyware is a form of malicious software and its capabilities allow it to covertly infiltrate devices to monitor and collect sensitive information on users. The fact that spyware gets downloaded without any action from the user – such as clicking on a phishing email, downloading unsecure software, and so forth – increases the possibility of a user unknowingly using a device hacked by spyware, making it much more concerning than other malware.

The NSO Group's Pegasus Spyware gained attention following investigations by Amnesty International and Citizen Lab, which revealed the NSO Group's contracts with numerous governments around the world and the use of Pegasus to target opposition politicians, journalists and activists.[1] Less spoken about, however, is the growing global spyware market and demand for such malware, as well as the lack of regulation against it.

With at least 18 different companies such as Intellexa, Gamma Group, FinFisher, Cytrox and more, the industry is estimated at USD 12 billion, with at least 3,111 individuals having been targeted by such spyware since 2015.[2] A report by Carnegie Endowment for International Peace reveals that spyware firms hold contracts with over 74 governments, spanning from democracies to authoritarian regimes.[3] Given the difficulties with tracking the spyware market it's hard to quantify exact percentages but Carnegie's dataset showed a rough split of 43% to 56%, with authoritarian states leading slightly in contract numbers. The application of these spyware products, once labeled as tools for counterterrorism and crime prevention, has morphed into a global concern as both authoritarian and democratic regimes exploit them to monitor and suppress domestic dissent. Most recently, Greece made headlines for its use of the spyware Predator as the ruling party came under suspicion of illegally targeting opposition leaders, journalists, and civic leaders.[4]

Recent investigations underscore the willingness of spyware companies to turn a blind eye to how their tools are deployed. In an undercover investigation by Al Jazeera, prominent European spyware firms were found willing to work with sanctioned groups, even offering ways to conceal the illegal

[1] Ronald J. Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy", Foreign Affairs, December 22, 2022 https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

[2] Samuel Woodhams, "The Global Spyware Market Index.", Top10VPN, May 12, 2021 https://www.top10vpn.com/research/global-spyware-market-index/

[3] Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.", Carnegie Endowment for International Peace, March 14, 2023 https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

[4] Hendrik Mildebrath, "Greece's Predatorgate.", European Parliament, September, 2022 https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

transactions.[5] The Electronic Frontier Foundation published a report detailing spyware companies actively collaborating with authoritarian regimes to target dissidents. Notably, Italian firm Area SpA constructed monitoring centers for the Syrian regime in 2011 during the Arab Spring democracy protests.[6] Amidst these revelations, lesser-known players like Circles, linked to the NSO Group, have come under scrutiny for providing technology enabling governments to track individuals through their mobile phones.[7] There is also a growing number of online threat groups such as BlackOasis that are speculated to be customers of well-known spyware firms. Despite investigations and public outcry, the market resilience of spyware-as-as-service is evident.[8] While Area SpA faced an investigation and FinFisher eventually shut down, Hacking Team was bought by another company and rebranded to Memento Labs.[9] [10] [11] Even the NSO Group which is currently sanctioned by the U.S. Government is staging a comeback.[12]

The rapid surge in demand for spyware-as-a-service, coupled with inadequate regulation, has fuelled a gold rush mentality within the industry, where profit margins often supersede ethical concerns. Spyware-as-a-service companies maintain compliance with local regulations, but the secretive nature of the industry makes the verification of compliance challenging. Leading firms like FinFisher and Hacking Team have faced scandals and legal charges, caught selling to countries they explicitly denied dealing with or were prohibited from due to sanctions.[13] [14] Countries evading bans on direct spyware purchases employ indirect channels, leading to a cat-and-mouse game that undermines the effectiveness of restrictions. These indirect channels range from countries utilizing shell companies (a company used to hold funds and hide financial transactions for another business) or third-party trading intermediaries in countries not facing sanctions. Nations such as Iran and Syria, known for stifling dissent, exploit intermediaries to access advanced surveillance tools, effectively circumventing imposed bans.[15] The dynamics of this secretive industry make it difficult for governments, regulators, and advocates to effectively craft legislation and police the distribution of such technology.

[5] Simon Boazman, "How We Revealed the Surveillance World's Illegal Trades.", Al Jazeera, April 10, 2017 https://www.aljazeera.com/features/2017/4/10/how-we-revealed-the-surveillance-worlds-illegal-trades

[6] Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor.", Electronic Frontier Foundation, March 05, 2012 https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa

[7] Bill Marczak, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles", The Citizen Lab, December 01, 2020 https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[8] "BlackOasis, MITRE ATT&CK https://attack.mitre.org/groups/G0063/

[9] Katherine Walla, "Spyware Like Pegasus Is a Warning: Digital Authoritarianism Can Happen in Democracies, Too.", Atlantic Council, June 21, 2022 https://www.atlanticcouncil.org/blogs/new-atlanticist/spyware-like-pegasus-is-a-warning-digital-authoritarianism-can-happen-in-democracies-too/

[10] Ryan Gallagher, "German Spyware Vendor FinFisher Claims Insolvency Amid Investigation.", Bloomberg, March 28, 2022 https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation

[11] Lorenzo Franceschi-Bicchierai, "Hacking Team's New Owner: 'We're Starting From Scratch.", Vice, April 18, 2019 https://www.vice.com/en/article/neavnm/hacking-team-new-owner-starting-from-scratch

[12] Vas Panagiotopoulos, "Notorious Spyware Maker NSO Group Is Quietly Plotting a Comeback.", Wired, January 24, 2024 https://www.wired.com/story/nso-group-lobbying-israel-hamas-war/

[13] Katie Collins, "Hacking Team's Oppressive Regimes Customer List Revealed in Hack.", Wired, July 06, 2015 https://www.wired.com/story/hacking-team-spyware-company-hacked/

[14] "Charges Brought Against Former FinFisher Group CEOs.", Reporters Without Borders, May 31, 2023 https://rsf.org/en/charges-brought-against-former-finfisher-group-ceos

[15] Al Jazeera Investigative Unit, "Exclusive: Spyware firms in breach of global sanctions", Al Jazeera, April 10, 2017 https://www.aljazeera.com/news/2017/4/10/exclusive-spyware-firms-in-breach-of-global-sanctions

As the spyware industry continues to expand, the question remains if and how this invasive technology is to be regulated. Spyware's prevalence in digital spaces, poses a growing impediment to digital privacy and individual freedoms. President Joe Biden's recent executive order on spyware marks a significant step towards regulating that market.[16] However there is still a significant gap in the international regulations governing spyware companies and their sales. The E.U, while demonstrating growing concern of spyware's usage, especially within its member states, is still slow to develop official legislation.[17] There are persistent challenges of enforcing limited legal guidelines around spyware and addressing the growing use of its technology by governments, both authoritarian and democratic.

[16] "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security.", 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/

[17] Romain Bosc and Charles Martinet, "Europe Vs. Spyware.", German Marshall Fund of the United States, https://www.gmfus.org/news/europe-vs-spyware

Section 2

Risk Outlook for 2024

1. Chilling effect on speech and suppression of press freedom

Governments can make use of spyware to monitor the activities of journalists, activists, researchers, and politicians, as well as extract data from their devices.[18] For instance, in 2015, Mexican journalist Carmen Aristegui and a family member were sent Pegasus exploit links while investigating corruption involving the then-Mexican President Enrique Peña Nieto.[19] It was also already reported that critics of the governments of Serbia, Russia, Spain, Poland and other countries were targeted by spyware, even if they may not live in the country.[20] [21] [22] [23] This implies a transnational suppression of freedom of expression and could reduce opposition to injustice in the forms of protests, vocal criticisms, and investigative journalism, etc. Such a chilling effect on targets will eventually undermine government accountability.[24]

2. Democracy and human rights credibility

As noted above, 43% of the 74 states that contracted commercial firms to provide spyware were democracies. In addition, data collected by Carnegie's global inventory of commercial spyware and digital forensics shows that end-users from at least 14 EU member states purchased Pegasus between 2011 and 2023.[25] Export control agencies usually regard EU member states as sufficiently guaranteeing

[18] "Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally.", Amnesty International, July 19, 2021 https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[19] Ronald J. Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy.", Foreign Affairs, December 22, 2022 https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

[20] Stephanie Kirchgaessner, "Critics of Serbia's Government Targeted With 'Military-Grade Spyware.", The Guardian, November 29, 2023 https://www.theguardian.com/technology/2023/nov/28/critics-of-serbias-government-targeted-with-military-grade-spyware

[21] Stephanie Kirchgaessner, "Russian News Outlet in Latvia Believes European State Behind Phone Hack.", The Guardian, September 25, 2023 https://www.theguardian.com/world/2023/sep/25/latvia-russia-meduza-phone-hack-galina-timchenko

[22] "Spain: Pegasus Spyware Scandal Reveals Risk of Intelligence Services Acting With Total Impunity.", Amnesty International, August 10, 2023 https://www.amnesty.org/en/latest/news/2022/05/spain-pegasus-spyware-scandal-reveals-risk-of-intelligence-services-acting-with-total-impunity/

[23] "Pegasus and similar spyware and secret state surveillance", Council of Europe, September 20, 2023 https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68

[24] "The impact of Pegasus on fundamental rights and democratic processes", European Parliament, January 2023 https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

[25] Steven Feldstein and Brian Kot, "Global Inventory of Commercial Spyware & Digital Forensics.", Mendeley Data, March 02, 2023 https://doi.org/10.17632/csvhpkt8tm.10

the highest human rights standards, exempting EU countries from further human rights due diligence.[26] But the above data shows that even the most human-rights-compliant countries, regardless of the type of regime, are prone to spyware abuse in the absence of adequate safeguards and supervision or insufficient supervision.

3. Infiltrating opposition, especially during elections

Governments can use spyware to target opposition figures to influence election outcomes. One of the most shocking cases occurred in Spain, a parliamentary democracy and EU member state.[27] Citizen Lab discovered that, from 2017 to 2020, Pegasus was used to tap into most of the content of Catalan civil society and government. These targets included every member of the European Parliament from Catalonia who supported Catalan independence, every president of Catalonia since 2010, and many members of the Catalan legislature, including several presidents of the Catalan Parliament. 70 countries are going to hold elections in 2024, including several major economic powers, such as the US and India, but also ones of strategic importance, such as South Korea, where spyware may be used in attempts to target political oppositions and civil dissidents to alter these countries political fates.[28]

4. Countering Geopolitical Rivals

Spyware can also influence the geopolitical landscape if it is used to target adversaries. An investigation found that NSO agreements helped Israeli Prime Minister Benjamin Netanyahu sign the Abraham Accords with Bahrain, Morocco, and the UAE.[29] In turn, states not only use Pegasus to counter opposition groups, journalists, and non-governmental organizations (NGOs) but also to target geopolitical rivals. NordVPN ranks the US as the 5th country with the highest risk of cybercrime, while the UK is 10th, and northern Europe is rated as the most vulnerable region in the world to cybercrime due to widespread usage of digital services and devices. This makes Western nations particularly vulnerable to the use of spyware by its adversaries for geopolitical goals.[30]

5. Use of spyware in conflict

In conflict settings, spyware facilitates the acquisition of valuable intelligence by being able to penetrate encrypted networks and devices without being detected, making it a very sophisticated

[26] Steven Feldstein and Brian (Chun Hey) Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.", Carnegie Endowment for International Peace, March 14, 2023 https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

[27] Ronald J. Deibert, "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy.", Foreign Affairs, December 22, 2022 https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

[28] Koh Ewe, "The Ultimate Election Year: All the Elections Around the World in 2024.", TIME, December 28, 2023 https://time.com/6550920/world-elections-2024/

[29] Aluf Benn, "Netanyahu Used NSO's Pegasus for Diplomacy. Now He Blames It for His Downfall - Israel News.", Haaretz, February 05, 2022 https://www.haaretz.com/israel-news/2022-02-05/ty-article/.premium/netanyahu-used-nsos-pegasus-for-diplomacy-now-he-blames-it-for-his-downfall/0000017f-e941-dc91-a17f-fdcd55c80000

[30] "Cyber Risk Index", NordVPN, https://nordvpn.com/cri/

intelligence gathering tool. Adversaries could steal intelligence data to make strategic decisions that will lead them to a strategic advantage. Access Now documented the first-ever use of spyware in conflict where Anna Naghdalyan, a former spokesperson for the Armenian Foreign Ministry who had intimate knowledge of the ceasefire negotiations between Armenia and Azerbaijan was targeted by spyware.[31] The Israeli military has reportedly been using Pegasus spyware to tap phones of suspected Hamas militants in the ongoing Israel-Hamas conflict.[32]

6. Use of spyware in financial crime

Spyware can also open the door for further data breaches like double extortion. Double extortion, often also referred to as ransomware, refers to the practice of threatening to release stolen data unless the victim makes a payment.[33] Cybercriminals are increasingly using spyware to target individuals, businesses and governments, primarily to steal data facilitating financial crimes.[34] While the NSO Group states that it only collaborates with states, other spyware firms are likely to act on the cybercriminals' increasing demand for the malware, which would only expand and facilitate domestic and international financial crime.

[31] Vittoria Elliott, "Pegasus Spyware Is Detected in a War Zone for the First Time.", Wired, May 25, 2023 https://www.wired.com/story/pegasus-spyware-war-zone-first-time/

[32] Jason Blessing, "A notorious Israeli spyware firm wants to use the Gaza war to make a comeback", The Hill, January 27, 2024 https://thehill.com/opinion/cybersecurity/4433419-a-notorious-israeli-spyware-firm-wants-to-use-the-gaza-war-to-make-a-comeback/

[33] "#StopRansomware Guide", Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/stopransomware/ransomware-guide

[34] "Spyware", Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf

Section 3

Policy Recommendations

1. Enhanced Awareness of Digital Hygiene

Spyware inherently relies upon human error – be it a faulty password, a nefarious link, or even using non-updated software[35]. Politically exposed persons must be made aware of their personal risks when interacting online, and take steps to negate this. Indeed, many of the ways of protecting your device from Pegasus spyware are simple in their approach. As a result, **greater institutional emphasis must be placed upon education of those working in the public sphere**, whilst personal responsibility for personal digital interactions must be taken.

"greater institutional emphasis must be placed upon education of those working in the public sphere"

2. Development of National Institutions preventing the deployment of spyware unlawfully

Constraining governments against the use of spyware inherently relies upon the legitimate legislation against its use. The development of institutions protecting citizens against its unlawful application is a key area to regulate the industry. Whilst spyware can be deployed legitimately, for instance in cases of national security, preventing its unlawful application relies on strong public bodies and rigorous governance. Indeed, the blurred lines between lawful and unlawful use of spyware was made obvious in Greece, where the Prime Minister whilst admitting the use of spyware was "politically unacceptable", it was still technically legal[36]. As a result, the **development of national agencies regulating the use of spyware** is needed to protect democratic expression.

3. Development of Vigorous Civil Groups

Reformed spyware governance must acknowledge the limitations of governmental reform, as whilst governments and the international community can limit the proliferation of spyware, they cannot be

[35] "Cyber Hygiene - Digital Hygiene.", Digital Hygiene, https://digitalhygiene.net/

[36] "Greek PM Takes Heat Over Phone Tapping Scandal, Defends Spy Service's Work.", Reuters, August 26, 2022 https://www.reuters.com/world/europe/greek-pm-takes-heat-over-phone-tapping-scandal-defends-spy-services-work-2022-08-26/

trusted implicitly[37]. As a result, **strong civil society groups capable of monitoring governments are key** to both preventing infringements and holding governments accountable. Indeed, the breaking of the Pegasus Scandal by two civil society groups – Amnesty International Security Lab and Forbidden Stories – has highlighted the instrumental role of civil society in monitoring of spyware use. Governments and international organizations should extend support for creating and sustaining such civil society groups.

4. Effective International Legislation and monitoring against spyware exports

The Pegasus scandal has proved that democracies can also be susceptible to both the use and the manufacturing of politically motivated spyware. Whilst heightened government awareness of these risks has resulted in some legislation, these policies have been haphazard in their success against global trade in commercial spyware. [38] [39] [40] Both nations and the wider interactional community are still struggling to adequately prosecute actors in the spyware trade. An example of this was the failure of Spanish courts to prosecute the use of Pegasus due to a "complete" lack of cooperation by the Israeli state.[41] As a result, heightened **international cooperation (alongside clear regulatory objectives) in both sanctioning and prosecuting spyware that violates fundamental rights, must become an internationally recognised norm.** In a similar manner to the development of the Wassenaar Arrangement which regulates conventional arms sales, new international agreements are needed to prevent the proliferation of the spyware services.

"international cooperation (alongside clear regulatory objectives) in both sanctioning and prosecuting spyware that violates fundamental rights, must become an internationally recognised norm"

5. Increased Monitoring to Tighten Export Gaps and patch technical vulnerabilities

Preventing the sale of commercial spyware is crucial to prevent its use, both domestically and internationally. Whilst UN officials called for an immediate moratorium on spyware sale in the aftermath of the Pegasus scandal, there is minimal support for this measure, due to spywares integration into many nations' security services. Furthermore, efforts to curb spyware market growth

[37] "Civil Society Can Help Ensure AI Benefits Us All. Here's How.", World Economic Forum, July 08, 2021 https://www.weforum.org/agenda/2021/07/civil-society-help-ai-benefits/

[38] Foreign, Commonwealth & Development Office, "Efforts to Counter the Proliferation and Misuse of Commercial Spyware: Joint Statement.", March 30, 2023 https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement

[39] "Fighting Cybercrime: New EU Cybersecurity Laws Explained", European Parliament, October 11, 2022 https://www.europarl.europa.eu/topics/en/article/20221103STO48002/fighting-cybercrime-new-eu-cybersecurity-laws-explained

[40] Zack Whittaker, "Biden Executive Order Bans Federal Agencies From Using Commercial Spyware.", TechCrunch, March 27, 2023 https://techcrunch.com/2023/03/27/biden-order-commercial-spyware-ban/

[41] "Spain Closes Pegasus Investigation Over 'Lack of Cooperation' From Israel.", The Guardian, July 10, 2023 https://www.theguardian.com/world/2023/jul/10/spain-closes-pegasus-investigation-over-lack-of-cooperation-from-israel

by sanctioning related entities and individuals have led to customers in search of the technology to use indirect channels as highlighted above, making it harder for states to continue to hold sanctioned entities accountable. **By strengthening partnerships with civil society groups, cybersecurity firms, and global law enforcement agencies** such as Interpol and Europol, **states could ensure more effective monitoring of spyware usage**. By more effectively sanctioning entities and individuals producing and purchasing spyware, such efforts could help ensure a mechanism of continued accountability which could both dissuade customers from purchasing spyware and curb incentives for market growth.

The application of spyware relies heavily upon continuous technical support, to mitigate future updates and the outstripping of their services by antivirus software[42]. However, a lack of information sharing between both states and private actors damages the ability to patch previously infiltrated systems. As a result, greater **transnational information sharing between both private and public entities** is required to crack down on the use of politically motivated spyware.

6. Mandating of Corporate Governance

78% of the world's spyware producers come from democracies in Europe, the Middle East and North America. International conventions such as the UN's Guiding Principles on Business and Human Rights demand adequate due diligence to prevent and mitigate human right violations [43], and these **states have a duty to update business legislation** and require technology companies to implement greater self-regulation to prevent the misuse of their services. States need to make a more consistent effort in increasing human rights due diligence through the implementation of **mandatory trade impact assessments with a human rights component**.

[42] Arielle Waldman, "Citizen Lab Details Ongoing Battle Against Spyware Vendors.", Tech Target, January 29, 2024 https://www.techtarget.com/searchSecurity/news/366568215/Citizen-Lab-details-ongoing-battle-against-spyware-vendors

[43] "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework.", The Office of the High Commissioner for Human Rights, January 01, 2012 https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

LONDON POLITICA