PRIORITY ISSUE:

Commercial Spyware Threatening Journalists

Advisory Note by the High Level Panel of Legal Experts on Media Freedom

23 June 2026

This Advisory Note:

I. Reviews the crisis and threat to media freedom involving commercial spyware;
II. Sets out responses thus far by countries, civil society, the private sector and other stakeholders to counter the threat; and
III. Offers recommendations for concrete action moving forward.

1. The High Level Panel of Legal Experts on Media Freedom issues this Advisory Note to focus attention to the unprecedented threat posed to journalists and human rights defenders by the abuse of commercially available spyware technologies. Globally, the targeting of independent journalists through harassment, intimidation, and violence has reached crisis levels.[1] Strategic technologies, including commercial spyware and other surveillance technology, have contributed to this dangerous targeting and silencing of journalists.[2] These technologies have been abused to monitor or track journalists and human rights defenders, facilitating harassment, unlawful invasions of privacy, physical violence, and even assassination.[3]

2. The countries that are members of the Media Freedom Coalition ("MFC") are uniquely placed to promote and protect media freedom within the United Nations and regional frameworks in the face of these pressing challenges. This Advisory Note provides a brief overview of the problem and responses thus far before concluding with a set of recommendations for countries and stakeholders to counter the urgent threat to media freedom posed by the proliferation and abuse of commercial spyware. When this Note refers to the "abuse" of commercial spyware, it means any use of such technologies that fails to take into account and uphold international human rights standards, including instances in which the technology is used for unlawful or illegitimate purposes, as well as ostensibly legitimate uses for law enforcement or national security purposes without adherence to the rule of law (including appropriate judicial oversight) and applicable international legal principles.

I. PROLIFERATION OF THE USE OF COMMERCIAL SPYWARE TO LIMIT MEDIA FREEDOM

3. **Advancements in Commercial Spyware.** Recent advances in commercial spyware technology have accelerated an already concerning trend of targeting journalists and other human rights defenders, including by strengthening tools sold as part of the "hacker-for-hire" industry.[4] A particularly important and malicious example is so-called "zero-click spyware," which allows an attacker to remotely access and control a smartphone without the user having to click a link as in a traditional malware attack.[5] Infections of this type enable hackers to obtain the files, messages, and location data of an infected smartphone and to spy on the smartphone's user by activating the microphone and camera.[6]

4. **Proliferation of Commercial Spyware.** Years of investigations have confirmed widespread abuse of commercial spyware to profile journalists, political dissidents, and human rights defenders.[7] While there are many versions of these technologies, two high-profile examples are Pegasus, created by Israel-based NSO Group, and Predator, developed by North Macedonia-based Cytrox, part of the Intellexa alliance.[8] Public

reports suggest that Pegasus has been used in at least 45 countries around the world, in authoritarian and democratic countries alike, Predator customers are suspected in at least 11 countries, and Intellexa alliance products are in use in 25 or more countries.[9]

5. **Targeting of Journalists.** Journalists have become an all-too-frequent target of commercially available surveillance spyware.[10] More than 180 journalists in 21 countries are known to have been tracked with Pegasus, but the true number is likely much higher.[11] Some of the most high-profile cases are those of Jamal Khashoggi (Saudi Arabia/United States, Washington Post), Lenaïg Bredoux (France, Mediapart), and Siddharth Varadarajan (India, The Wire).[12] As the Secretary General of Amnesty International described in the aftermath of the murder of Mr. Khashoggi, "[d]etermining whether his phones had been hacked, whether he was under digital surveillance, identifying the spyware—these are all crucial elements both for the purpose of truth-telling and for understanding and preventing the targeting of dissidents."[13] More recent publicly reported cases include Jelena Veljković (Serbia, BIRN), Francesco Cancellato and Ciro Pellegrino (Italy, Fanpage.it), and Teixeira Cândido (Angola, Jornal de Angola). These recent examples underscore the threat to journalists posed not only by Pegasus but also by other commercial spyware tools such as Paragon's Graphite and Intellexa's Predator.[14]

6. The right to report freely and safely is a pillar of democracy protected by international human rights law, including through guarantees of freedom of expression and freedom of association. The targeting of journalists with commercial spyware is especially dangerous because it compromises confidential sources, chills investigative reporting, and undermines the press's ability to expose corruption, human rights abuses, and other matters of public interest. Spyware tools have also been deployed disproportionately against women, who face highly sexualized harassment intended to intimidate and silence them.[15]

II. RESPONSES TO COUNTER THE IMPROPER USE OF COMMERCIAL SPYWARE

7. **Civil Society Efforts.** Civil society and media organizations have been on the front lines of this issue for years, including by uncovering and exposing specific users and targets of commercial spyware, as well as the reach of Pegasus and Predator more broadly.[16] The work of these organizations has been critical in focusing public attention on commercial spyware as a threat to journalists, politicians, and human rights defenders around the world.[17]

8. For example, the Pegasus Project—a collaboration of more than 80 journalists from 17 media organizations in 10 countries—identified more than 50,000 potential Pegasus victims, including journalists, human rights activists, and lawyers across Asia, Central America, Europe, and Africa, as well as approximately a dozen client governments.[18] Several countries, including Mexico, Germany, Hungary, Poland, Spain, and Israel, later confirmed purchases of Pegasus.[19] These investigations helped prompt demonstrations in Hungary and India and judicial or parliamentary inquiries in Spain, Hungary, Poland, Mexico, and the European Parliament.[20]

9. The Predator Files investigation likewise tracked sales of surveillance technologies to Egypt, Libya, Madagascar, Saudi Arabia, Vietnam, France, and other countries.[21] Citizen Lab and Meta have documented suspected Predator customers across the Middle East, Europe, Africa, Asia, and the Americas.[22] Amnesty International has also identified a surveillance campaign targeting senior officials in the European Parliament, European Commission, U.S. Congress, and United Nations, as well as journalists, researchers, and think tanks.[23] The Atlantic Council has further mapped 435 entities across 42 countries in the commercial spyware market, highlighting opaque supply chains and the heightened risk to journalists and civil society.[24]

10. In response to this crisis, civil society organizations and independent experts have called for a moratorium on the purchase, sale, transfer, servicing, and use of commercial spyware until human rights safeguards are in place, including through a 2021 open letter signed by 156 organizations and 26 experts.[25] The UN Working

Group on Business and Human Rights and the Special Rapporteurs on the promotion and protection of the right to freedom of expression and on the situation of human rights defenders have called for a similar moratorium.[26] In 2022, the civil society organization Access Now and the Government of Catalonia also presented the Geneva Declaration on Targeted Surveillance and Human Rights at a side event to the 51st session of the UN Human Rights Council.[27]

11. In addition to calling for greater legal oversight, civil society actors have provided technical support to individuals potentially facing abuse from surveillance technology. Citizen Lab and Amnesty International both assist individuals who believe they have been targeted,[28] including in Amnesty's case through its Mobile Verification Toolkit and Digital Forensics Helpline. Companies such as Trail of Bits and ZecOps offer related tools,[29] while Access Now provides a Digital Security Helpline for real-time technical assistance and advice to civil society organizations, journalists, and media organizations responding to cyber threats.[30]

12. **Private Sector Efforts.** Some companies in the technology industry have taken steps to address the proliferation of commercial spyware abuse. For example, in March 2024, Paladin, one of the biggest investors in cybersecurity startups, and several other venture capital firms published a set of voluntary investment principles.[31] These principles call for firms to invest in companies that "enhance the defense, national security, and foreign policy interests of free and open societies," and to ensure that the companies they invest in "only sell to countries that abide by international law as recognized by the United States."[32]

13. **Legal Proceedings.** Individuals, organizations, and technology companies around the world have also turned to courts in search of redress. According to Citizen Lab, at least 24 lawsuits are ongoing against NSO Group and/or countries alleged to have used Pegasus.[33] These proceedings have been initiated in the United Kingdom, United States, Spain, France, Hungary, Cyprus, Israel, and elsewhere against the Group and have involved countries including Israel, Bahrain, Spain, Hungary, Morocco, the United Arab Emirates, and Saudi Arabia.[34] Additional complaints have been filed with the European Commission and referred to UN Special Rapporteurs.[35] Notably, in May 2025, the U.S. District Court for the Northern District of California ordered NSO Group to pay $167 million in damages to Meta after Pegasus was found to have been used to illegally hack 1,400 WhatsApp accounts belonging to journalists, human rights activists, and officials.[36] And in February 2026, Polish prosecutors charged two former intelligence chiefs in connection with the authorization and use of Pegasus without required security accreditation, as part of a broader domestic investigation into alleged spyware abuse.[37]

14. Regional human rights bodies have also addressed the issue. In March 2022, the Inter-American Commission on Human Rights held a hearing on cyber-surveillance in El Salvador and incorporated the issue into its monitoring of the country. While calling for an immediate moratorium on the sale, transfer, and use of surveillance technology until adequate human rights safeguards are in place, the Commission stressed that communications-device tapping must rest on a transparent legal framework, and comply with international human rights standards, including the requirements of necessity, proportionality, and a legitimate aim.[38] In October 2025, the Inter-American Commission on Human Rights Special Rapporteurship concluded that digital surveillance poses a systemic, existential threat to journalists in the Americas, documenting the targeting of media in Mexico, El Salvador, the Dominican Republic, and Colombia, including hacking, monitoring, forced exile, and infections closely linked to reporting on corruption, organized crime, and abuses.[39] The European Court of Human Rights has also been asked to consider cases concerning alleged Pegasus surveillance, and more than two dozen applications have been filed in recent years.[40]

15. **Country Action.**

    a. **Restrictions on Use.** Some countries have made public commitments to investigate or restrict the use of commercially available surveillance spyware. Costa Rica, for example, has called for an "immediate moratorium on the use of spyware technology until a regulatory framework that protects human rights is implemented."[41] The European Parliament established the Pegasus Committee in March 2022 to investigate the use of Pegasus and equivalent spyware in EU member countries, and

the Committee later called for an immediate moratorium on the sale, acquisition, transfer, and use of spyware.[42]

b. Countries have also entered into multilateral commitments: on March 30, 2023, Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States released a Joint Statement on efforts to counter the proliferation and misuse of commercial spyware.[43] Finland, Germany, Ireland, Japan, Poland, and South Korea joined on March 18, 2024, followed by Austria, Estonia, Lithuania, and the Netherlands on September 22, 2024.[44] Separately, in 2018, G7 countries established the Rapid Response Mechanism to address foreign threats to democracy, including technology-enabled suppression of independent voices, information warfare, and manipulation of democratic processes.[45]

c. At the same time, there have been notable instances of back tracking; for example, while the United States issued an executive order in March 2023 prohibiting departments and agencies from operationally using commercial spyware where credible information indicates significant counterintelligence, security, or improper-use risks, the Trump Administration reportedly reactivated a previously suspended contract with Paragon in September 2025.[46]

d. **Export Controls.** The non-binding Wassenaar Arrangement encourages its 42 participating countries to enforce stronger controls on transfers of selected items, including "intrusion software" and "IP network surveillance systems," through domestic export-licensing regimes.[47] Similarly, the EU's Recast Dual-Use Regulation, in force since November 9, 2020, introduced authorization requirements for exports of cybersurveillance tools used or intended for use in connection with internal repression or serious violations of human rights and international humanitarian law.[48] On December 10, 2021, Australia, Denmark, Norway, and the United States launched the Export Controls and Human Rights Initiative, committing to a voluntary written code of conduct to guide export controls in compliance with international human rights law.[49] The Venice Commission likewise called for robust export controls and for licenses conditioned on compliance with human rights standards in December 2024.[50]

e. **Guiding Principles.** In March 2023, the 36 member countries of the Freedom Online Coalition published the voluntary and non-binding Guiding Principles on Government Uses of Surveillance Technologies, calling on governments to ensure appropriate legal protections for domestic law enforcement uses of surveillance technology; respect human rights; avoid discrimination; apply principles of lawfulness, necessity, proportionality, and reasonableness; and ensure oversight, accountability, transparency, and adequate training for government officials.[51] In parallel, the United Kingdom and France launched the Pall Mall Process, a global initiative involving governments, industry, civil society, and academia to confront the proliferation and misuse of commercial spyware, in February 2024.[52] By early 2025, 25 countries—including the United States, United Kingdom, 17 EU member countries, Ghana, Japan, Kosovo, Moldova, South Korea, and Switzerland—had endorsed its Code of Practice for States, committing to accountability, precision, oversight, and transparency in the development, purchase, and export of intrusion tools.[53]

f. In 2024, the Venice Commission also set out minimum guiding principles for spyware, emphasizing safeguards under domestic law to limit the scope, duration, target, and purpose of surveillance; judicial authorization based on a least-intrusive-means test; heightened protection for journalists, lawyers, and others protected by professional privilege; independent oversight, post-surveillance notification where feasible, and destruction of data once investigations conclude.[54]

16. **Continued Proliferation.** Despite these efforts, commercial spyware continues to proliferate with too few regulatory checks in place to ensure the protection of journalists and human rights defenders. Notably, in April 2026, the U.S. Department of Homeland Security acknowledged it is using spyware tools, reportedly including Paragon's "Graphite," to intercept encrypted communications in investigations targeting fentanyl-trafficking

organizations.[55] Similarly, in Europe, a proposed Communications (Interception and Lawful Access) Bill in Ireland reportedly would create a legal basis for Irish police to use covert surveillance technologies, including commercial spyware, to access encrypted communications, while civil society experts have warned that Ireland lacks sufficiently clear oversight, intelligence-law safeguards, and limits on "national security" discretion to prevent abuse.[56]

III. HIGH LEVEL PANEL RECOMMENDATIONS

17. The High Level Panel takes note of the call by many civil society organizations and UN representatives for a moratorium on the use of this kind of technology until adequate legal safeguards have been put in place, and is of the further view that, even as discussions of a moratorium continue, countries should take immediate steps to address the abuse of these technologies to suppress media freedom.

18. To address the ongoing and urgent crisis of the cyber targeting of journalists and human rights defenders, the High Level Panel recommends that countries, including the member countries of the MFC, designate this issue a high-level policy priority and:

    1. **Commit to imposing strict legal requirements on any procurement and use of commercial spyware** in accordance with human rights, fundamental freedoms, and other norms of international law, with an emphasis on identifying and avoiding such use where it poses significant risk of infringing freedoms of expression or association;

    2. **Enforce requirements on companies** that develop commercial spyware to incorporate safeguards throughout the product lifecycle to prevent abuse and to take necessary steps to prevent commercial spyware from being sold to actors who abuse it;

    3. Take steps to give effect to an **international rapid response mechanism**, including by establishing and working within such mechanisms as the G7 Rapid Response Mechanism, to track and coordinate information relating to validated instances of cyber targeting of journalists and human rights defenders for the purpose of identifying opportunities for coordinated response and ensuring that information and analysis is shared efficiently among country partners and the public;

    4. **Support individual journalists and human rights defenders** who believe they have been targeted by the abuse of commercial spyware, including by committing technical and/or financial resources to civil society organizations working on these challenges;

    5. Encourage private sector and civil society actors to provide **technical and non-technical support** to those targeted by abuse of commercial spyware, including journalists and human rights defenders; and

    6. **Encourage investors** in technology companies that produce commercial spyware and surveillance software **to undertake due diligence and to exercise any leverage with the businesses in which they invest** to ensure such businesses are: (i) incorporating safeguards along the product lifecycle to prevent abuse, and (ii) taking necessary steps to prevent commercial spyware from being sold to actors who abuse these technologies.

NOTES

[1] Freedom House, "New Report: Governments Are Escalating Transnational Repression to Silence Journalists around the World," Press Release, Dec. 6, 2023, *available at:* https://freedomhouse.org/article/new-report-governments-are-escalating-transnational-repression-silence-journalists-around.

[2] UN Office of the High Commissioner for Human Rights, "Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns," Sept. 16, 2022, *available at:* www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report; U.S. Department of State, "U.S. Advances UN Recognition of Threats Posed by Commercial Spyware," Oct. 11, 2024, *available at:* https://2021-2025.state.gov/u-s-advances-un-recognition-of-threats-posed-by-commercial-spyware/?safe=1; Center for Democracy & Technology, "2024 Annual Report: Speaking Out Against Spyware Abuse," 2024, *available at:* https://cdt.org/2024-annual-report-speaking-out-against-spyware-abuse/.

[3] UN Office of the High Commissioner for Human Rights, "Use of spyware to surveil journalists and human rights defenders," Statement by UN High Commissioner for Human Rights Michelle Bachelet, July 19, 2021, *available at:* www.ohchr.org/en/press-releases/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high; Committee to Protect Journalists, "Spyware and Press Freedom," *available at:* https://cpj.org/spyware/.

[4] Security Week, "Spyware Find Highlights Depth of Hacker-for-Hire Industry," Dec. 17, 2021, *available at:* www.securityweek.com/spyware-find-highlights-depth-hacker-hire-industry/; The Bureau of Investigative Journalism, "Inside the Global Hack-for-Hire Industry," Nov. 5, 2022, *available at:* www.thebureauinvestigates.com/stories/2022-11-05/inside-the-global-hack-for-hire-industry/.

[5] Cyber Strategy Institute, "Zero Click Warfare: No User Needed Exploits & Zero-Click Attacks Demystified," May 14, 2025, *available at:* https://cyberstrategyinstitute.com/zero-click-warfare-no-user-needed-exploits-zero%E2%80%91click-attacks-demystified/.

[6] Parliamentary Assembly Resolution 2513, "Pegasus and Similar Spyware and Secret State Surveillance," 2023, *available at:* https://pace.coe.int/en/files/33116/html.

[7] Amnesty International, "The Pegasus Project," July 18, 2021, *available at:* https://securitylab.amnesty.org/latest/blog/2021/07/the-pegasus-project; Citizen Lab, "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Sept. 18, 2018, *available at:* https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.

[8] Citizen Lab, "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Sept. 18, 2018, *available at:* https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries; Amnesty International, "Global: "Predator Files" Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials," Oct. 9, 2023, *available at:* www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting/.

[9] Media Defence, "Module 4: Privacy and Security Online 19," 2024, *available at:* www.mediadefence.org/ereader/wp-content/uploads/sites/2/2022/12/Module-4-Privacy-and-security-online-2024, at 17; Amnesty International, "Global: "Predator Files" Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials," Oct. 9, 2023, *available at:* www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting/.

[10] Access Now, "Joint Statement: States Must Take Immediate Action to Stop Spyware Threatening Press Freedom," May 3, 2023, *available at:* www.accessnow.org/press-release/spyware-press-freedom-statement/; Citizen Lab, "Stopping the Press: New York Times Journalist Targeted by Saudi-Linked Pegasus Spyware Operator," Jan. 28, 2020, *available at:* https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/.

[11] Access Now, "Joint Statement: States Must Take Immediate Action to Stop Spyware Threatening Press Freedom," May 3, 2023, *available at:* www.accessnow.org/press-release/spyware-press-freedom-statement/.

[12] Citizen Lab, "The NSO Connection to Jamal Khashoggi," Oct. 24, 2018, *available at:* https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi/; Nice Matin, "Espionné par le Maroc via le logiciel Pegasus," Mediapart porte plainte, July 19, 2021, *available at:* www.nicematin.com/faits-divers/espionne-par-le-maroc-via-le-logiciel-pegasus-mediapart-porte-plainte-702918; Amnesty International, "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists," Dec. 28, 2023), *available at:* www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

[13] Times of Israel, "Khashoggi wife readying to sue Israel's NSO for alleged phone hacking," Sept. 23, 2022, *available at:* www.timesofisrael.com/khashoggi-wife-readying-to-sue-israels-nso-for-alleged-phone-hacking/.

[14] Amnesty International, "Serbia: Journalists targeted with Pegasus spyware," March 27, 2025, *available at*: https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/; Committee to Protect Journalists, "Italian investigative journalist Francesco Cancellato targeted with Paragon spyware," Feb. 10, 2025, *available at*: https://cpj.org/2025/02/italian-investigative-journalist-francesco-cancellato-targeted-with-paragon-spyware/; Amnesty International, "Angola: Prominent journalist hacked with Predator spyware," Feb. 18, 2026, available at: www.amnesty.org/en/latest/news/2026/02/angola-spyware/.

[15] UN Office of the High Commissioner for Human Rights, "Interlinkages between women's rights and digital technologies, civic space, data and privacy, and freedom of expression," EGM/STI/OP.5, Oct. 2022, *available at:* www.unwomen.org/sites/default/files/2022-12/OP.5_OHCHR.pdf.

[16] Citizen Lab, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Sept. 18, 2018, *available at:* https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries; Amnesty International, "The Pegasus Project," Security Lab, *available at:* https://securitylab.amnesty.org/case-study-the-pegasus-project/; Amnesty International, "The Predator Files: Caught in the Net," Oct. 2023, *available at:* www.amnesty.nl/content/uploads/2023/10/The-Predator-Files-report.pdf.

[17] Amnesty International, "The Pegasus Project," Security Lab, *available at:* https://securitylab.amnesty.org/case-study-the-pegasus-project/; Amnesty International, "Global: "Predator Files" Spyware Scandal Reveals Brazen Targeting of Civil Society, Politicians and Officials," Oct. 9, 2023, *available at*: www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting/.

[18] Amnesty International, "The Pegasus Project," Security Lab, *available at:* https://securitylab.amnesty.org/case-study-the-pegasus-project/; Forbidden Stories, "About the Pegasus Project," *available at:* https://forbiddenstories.org/about-the-pegasus-project/; Amnesty International, "The Pegasus Project," Security Lab, *available at:* https://securitylab.amnesty.org/case-study-the-pegasus-project/.

[19] Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally," July 19, 2021, *available at:* www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/; Parliamentary Assembly, "Pegasus and similar spyware and secret state surveillance," Doc. 15825, Sept. 20, 2023, *available at:* https://pace.coe.int/en/files/33018/html; PBS, "Mexico Says Officials Spent $61 Million on Pegasus Spyware, July 28, 2021, *available at:* www.pbs.org/newshour/world/mexico-says-officials-spent-61-million-on-pegasus-spyware; SecurityWeek, "Germany Admits Police Used Controversial Pegasus Spyware," Sept. 7, 2021, *available at:* www.securityweek.com/germany-admits-police-used-controversial-

pegasus-spyware/; Budapest Post, "Hungary Admits Buying Pegasus Spy Software," *available at:* https://budapestpost.com/hungary-admits-buying-pegasus-spy-software-transitions; Reuters, "Poland's Ruling Party Admits Security Services Bought Pegasus Spyware," Jan. 7, 2022, *available at:* www.reuters.com/world/europe/ruling-party-figures-say-poland-has-pegasus-spyware-2022-01-07; Politico, "Reports: Spain sacks intel chief over Pegasus scandal," May 10, 2022, *available at:* www.politico.eu/article/report-spain-sacks-intel-chief-over-pegasus-scandal/; The New Arab, "Israeli police admit using NSO spyware on citizens," Feb. 1, 2022, *available at:* www.newarab.com/news/israeli-police-admit-using-nso-spyware-citizens; The Guardian, "FBI confirms it bought spyware from Israel's NSO Group," Feb. 2, 2022, *available at:* www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware.

[20] PBS, "Hungarians Protest Over Alleged Government Spying," July 26, 2021, *available at:* www.pbs.org/newshour/world/hungarians-protest-over-alleged-government-spying; Human Rights Watch, "India: Spyware Use Violates Supreme Court Privacy Ruling," Aug. 26, 2019, *available at:* www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling; Center for International Governance Innovation, "The Growing Global Spyware Industry Must Be Reined In," 2023, *available at:* www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/; *See* Reuters, "Spain Reopens Israeli Spyware Probe, Sharing Information With France," Apr. 23, 2024, *available at:* www.reuters.com/technology/cybersecurity/spain-reopens-israeli-spyware-probe-sharing-information-with-france-2024-04-23/; Euractiv, "Pegasus Scandal: Hungarian Prosecutor Investigating," July 22, 2021, *available at:* www.euractiv.com/section/politics/short_news/pegasus-scandal-hungarian-prosecutor-investigating/; The Guardian, "Poland Launches Inquiry Into Previous Government's Spyware Use," Apr. 1, 2024, *available at:* www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use; Heise, "Mexico: Investigation Into Alleged Bribe Payment for the Purchase of Pegasus Spyware," July 2025, *available at:* www.heise.de/en/news/Mexico-Investigation-into-alleged-bribe-payment-for-the-purchase-of-Pegasus-10483505.html; European Parliament Think Tank, "What Action Has Parliament Taken Against Spyware Abuse?," June 2, 2024, *available at:* https://epthinktank.eu/2024/06/02/what-action-has-parliament-taken-against-spyware-abuse.

[21] Amnesty International, "The Predator Files: Caught in the Net – The Global Threat from "EU Regulated" Spyware," 2023, *available at:* www.amnesty.eu/wp-content/uploads/2023/10/Executive-Summary_Predator-Files_English-1.pdf.

[22] *Id.*

[23] *Id.*

[24] Atlantic Council, "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights," *available at:* www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

[25] Amnesty International, "Joint Open Letter by Civil Society Organizations and Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer and Use of Surveillance Technology," July 27, 2021, *available at:* www.amnesty.org/en/documents/doc10/4516/2021/en/.

[26] UN Office of the High Commissioner for Human Rights, "Spyware Scandal: UN Experts Call for Moratorium on Sale of 'Life Threatening' Surveillance Tech," Aug. 12, 2021, *available at*: www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[27] Access Now, The Geneva Declaration on Targeted Surveillance and Human Rights, *available at:* www.accessnow.org/press-release/geneva-declaration-on-targeted-surveillance-and-human-rights/.

[28] Amnesty International, "Support Against Digital Attacks: How the Security Lab Can Help," Security Lab, May 29, 2024, *available at:* https://securitylab.amnesty.org/latest/2024/05/support-against-digital-attacks-how-the-security-lab-can-help/.

[29] Amnesty International, "Mobile Verification Toolkit (MVT)," Security Lab, *available at:* https://docs.mvt.re/en/latest/; Trail of Bits, "Introducing iVerify, the Security Toolkit for iPhone Users," Nov. 14, 2019, *available at:* https://blog.trailofbits.com; ZecOps, "NSO Exploits Still Remain Mysterious: ZecOps Can Help You Fight Back," *available at:* www.zecops.com.

[30] Access Now, "Digital Security Helpline," *available at:* www.accessnow.org/help/.

[31] Paladin Capital Group, "Paladin Capital Group Introduces Principles and Commitments to Prioritize National Security in Tech Investing During Meeting with White House," Press Release, Mar. 7, 2024, *available at:* www.paladincapgroup.com/paladin-capital-group-introduces-principles-and-commitments-to-prioritize-national-security-in-tech-investing-during-meeting-with-white-house/; Paladin Capital Group, "Investment Principles and Commitments on Trust, Safety, and Security," *available at:* www.paladincapgroup.com/investment-principles-and-commitments/.

[32] "Investment Principles and Commitments on Trust, Safety, and Security," *available at*: https://paladincapgroup.com/investment-principles-and-commitments/.

[33] Citizen Lab, "Litigation and Other Formal Complaints Related to Mercenary Spyware," Dec. 12, 2018, *available at:* https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

[34] *Id.*

[35] *Id.*

[36] *Id.*; Reporters Without Borders, "NSO/Pegasus: 17 Journalists from 7 Countries Join RSF's Complaint in Paris and Before the UN," Aug. 5, 2021, *available at:* https://rsf.org/en/nsopegasus-17-journalists-7-countries-join-rsf-s-complaint-paris-and-un.

[37] National Prosecutor's Office, "Charges of neglect of duty against former heads of the Internal Security Agency and the Military Counterintelligence Service in the Pegasus investigation," Feb. 25, 2026, *available at:* www.gov.pl/web/prokuratura-krajowa/zarzut-abw-skw.

[38] Nina Lakhani, "Human rights officials call for Pegasus spyware ban at El Salvador Hearing," Guardian, Mar. 17, 2022, *available at:* www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing.

[39] Inter-American Commission on Human Rights, "The Special Rapporteurship publishes its thematic report "The Impact of Digital Surveillance on Freedom of Expression in the Americas," Oct. 9, 2025, *available at:* www.oas.org/en/IACHR/jsForm/?File=/en/iachr/expression/media_center/preleases/2025/204.asp&utm_term=class-inft.

[40] European Court of Human Rights, Application no. 45877/22, Ganbarova v. Azerbaijan and 24 other applications, 24 Sept. 2025.

[41] Access Now, "Costa Rica: First Country to Call for a Moratorium on Spyware Technology," Apr. 13, 2022, *available at:* www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.

[42] European Parliament Decision 2022/480 on Setting Up a Committee of Inquiry to Investigate the Use of the Pegasus and Equivalent Surveillance Spyware, and Defining the Subject of the Inquiry, as Well as the Responsibilities, Numerical Strength and Term of Office of the Committee, Mar. 10, 2022.

[43] White House, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, Mar. 30, 2023, *available at:* www.govinfo.gov/content/pkg/DCPD-202300249/pdf/DCPD-202300249.pdf.
[44] White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," Mar. 18, 2024, *available at:* https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.
[45] G7, "Charlevoix Commitment on Defending Democracy from Foreign Threats," June 9, 2018, *available at*: www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-defending_democracy-defense_democratie.aspx?lang=eng.
[46] Access Now, "The U.S. Has Reactivated Its Paragon Contract—and It Should Alarm Everyone," Oct. 15, 2025, *available at:* www.accessnow.org/paragon-contract-spyware/.
[47] Wassenaar Arrangement Secretariat, Guidelines & Procedures, Including the Initial Elements 1 (2019), *available at:* www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf; Access Now, Wassenaar Arrangement Control List Additions for Surveillance Technologies 1–3 (2015), *available at:* www.accessnow.org/wp-content/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf.
[48] EU Regulation 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), 2021.
[49] The White House, "Joint Statement on the Export Controls and Human Rights Initiative," Dec. 10, 2021, *available at:* https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/12/10/joint-statement-on-the-export-controls-and-human-rights-initiative/.
[50] Council of Europe, Venice Commission, "Report on a Rule of Law and Human Rights-Compliant Regulation of Spyware," CDL-AD (2024)043, Dec. 13, 2024, *available at:* www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2024)043-e.
[51] Freedom Online Coalition, "Guiding Principles on Government Use of Surveillance Technologies," Mar. 2023, *available at:* https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf.
[52] Foreign Commonwealth and Development Office, "The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities," Feb. 6, 2024, *available at:* https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf.
[53] Alexandra Paulus, "Tackling the Proliferation of Cyber Intrusion Capabilities," Lawfare, June 4, 2025, *available at:* www.lawfaremedia.org/article/tackling-the-proliferation-of-cyber-intrusion-capabilities.
[54] Council of Europe, Venice Commission, "Report on a Rule of Law and Human Rights-Compliant Regulation of Spyware," CDL-AD(2024)043, Dec. 13, 2024, *available at:* www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2024)043-e.
[55] NPR, "ICE acknowledges it is using powerful spyware," Apr. 7, 2026, *available at:* www.npr.org/2026/04/07/nx-s1-5776799/ice-spyware-privacy.
[56] Tech Policy Press, "Ireland's New Surveillance Bill Opens Door to Spyware Abuse," Apr. 7, 2026, *available at:* www.techpolicy.press/irelands-new-surveillance-bill-opens-door-to-spyware-abuse/.