UNIVERSITY OF CALIFORNIA, IRVINE
BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

Written Testimony of David Kaye

Clinical Professor of Law
University of California, Irvine School of Law

Before a Hearing of the Senate Foreign Relations Committee
Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy

"Cyberspace under threat in the era of rising authoritarianism and global competition"

September 24, 2024

Chairman Van Hollen, Ranking Member Romney, Members of the Subcommittee:

Thank you very much for the invitation to appear before you today. My name is David Kaye. I am a law professor at the University of California, Irvine, School of Law, where I conduct research and teach courses in public international law, international human rights and humanitarian law, freedom of expression, and law and technology, and I direct the Law School's International Justice Clinic. I also serve as the U.S. Member of the European Commission for Democracy Through Law, the Venice Commission. From 2014 to 2020 I served as the United Nations (UN) Special Rapporteur on freedom of opinion of opinion and expression, and from 2020 to earlier this year I was the independent chair of the Board of the Global Network Initiative.

The Subcommittee has an opportunity to help develop national and global standards to control, counter and sanction abuse of the most intrusive technologies of the digital age, and I thank you for taking on this essential task for human rights and democracies worldwide.

Overview: Authoritarianism and the threat to "cyberspace"

Authoritarianism and global competition over the future of "cyberspace" are putting extraordinary strains on human rights, democracy and U.S. national security. Several states, led by China and Russia, are seeking to undermine the international human rights framework that is at the foundation of global democracy. They seek to redefine the very norms that have been at the center of the global value system since Eleanor Roosevelt led the negotiation of the Universal Declaration of Human Rights over seventy-five years ago. They aim to impose the state's authority over the internet in ways that are fundamentally at odds with the idea that digital space should strengthen civil society and promote freedom of expression, access to information and public participation in the life and politics of one's nation. They wage this effort in the major global forums of the day, including but not limited to the UN Human Rights Council and the negotiations for a Global Digital Compact and UN Cybercrime Convention.

As grave as the normative challenge in cyberspace is, it admittedly has an abstract quality to it. Not so on the technical and operational side, where the threats are tangible and the victims suffer serious harms. The old tactics, of course, have not disappeared. Contemporary authoritarian governments censor and criminalize criticism and dissent; intimidate, harass, jail and sometimes torture and kill journalists, human rights activists, and opposition figures; repress civil society organizations and weaponize the law and the concept of sovereignty to limit NGO activity.

The digital age has enabled states to turbocharge these tactics – and to do so at an ever decreasing cost. Why censor a mere newspaper or jam a radio transmission when you can order the internet to be shut down, or block a website or an app? Why engage in transparent public diplomacy when you can use disinformation and propaganda on social media? Why pursue the tedious work of physical surveillance or wiretapping when you can buy off-the-shelf technology to sweep up all of a person's digital footprint without their knowledge?

In my testimony, I will focus on one of these representative digital threats, commercial mercenary spyware, in part because it poses such severe and demonstrated risks not only to human rights and democracy but to national security. Congress and the Biden administration have taken world-leading steps to address the threat of commercial spyware, but there is much more to do, and that is why this hearing is so important. Therefore, I will first provide an overview of the nature of the threats posed by spyware to democracy, human rights and national security. I will then review steps that the United States and some within the international community are taking to address these grave threats. I will conclude with some broader remarks about the global threats and highlight steps the Senate should take to push an online rights-and-security agenda forward.

I. Spyware's threats to human rights and national security

In 2019, as UN Special Rapporteur, I reported on what seemed then to be a rapidly emerging threat of targeted digital surveillance.[1] At the time, I noted a range of digital attacks perpetrated by governments, often using tools supplied from a largely unregulated private industry. The report identified a range of serious attacks against human rights defenders, journalists and those simply in dissent, including by use of computer interference, commercial spyware and other forms of mobile device hacking, social engineering and phishing operations, network surveillance, abusive uses of facial and affect recognition, cell phone interception through tools known as IMSI catchers, and deep packet inspection.

Even then, it had become clear that commercial spyware was emerging as one of the gravest of all of these digital threats. Practically at the very moment that our lives had become persistently online, centered on devices that we all carry with us and that eventually lead back to the most personal details of our lives, careers, connections and opinions, an industry had arisen to intrude into our private spaces. It is an industry that develops exploits that take advantage of vulnerabilities in our devices, in turn providing governments with advanced capabilities allowing

[1] Report of the Special Rapporteur on Freedom of Opinion and Expression: Surveillance and Human Rights, A/HRC/41/35, May 28, 2019, *available at* https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur.

them to discretely, sometimes without even the requirement that a target click on a link or answer a call or message, install spyware on a mobile device, typically a smartphone. We can all imagine ourselves in the position of a victim: Spyware would give the attacker access to your text messages and phone calls, your photos and files, your contacts – indeed, everything on your device would be available to the attacker. Not only that, the possibility of microphone and camera access converts a device into "a bug in your pocket," as one analyst memorably put it.[2] The potential for abuse is obvious when made available without constraint to client governments unbound by the kinds of fundamental rules of law expressed in international human rights law or the U.S. Constitution's Fourth Amendment.

Beginning over a dozen years ago, The Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto began to put out report after report detailing uses of spyware against journalists, opposition figures, human rights defenders, and researchers, among others.[3] Since then, it has been joined by other non-government organizations, especially Amnesty Tech[4] and Access Now,[5] which have together demonstrated the use of spyware on every continent against the pillars of democratic life.

Given commercial spyware's extraordinary level of intrusiveness, the risks to fundamental rights are correspondingly severe. Human rights law – such as the International

---

[2] Written testimony of John Scott-Railton, Senior Researcher, the Citizen Lab, before the House Permanent Select Committee on Intelligence Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware", July 27, 2022.

[3] *See, e.g.*, Citizen Lab, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuous Proliferation," October 15, 2015, *available at* https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; Citizen Lab, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," August 24, 2016, *available at* https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Citizen Lab, "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," September 18, 2018, *available at* https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; Citizen Lab, "Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," December 16, 2021, *available at* https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; Citizen Lab, "GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement," July 17, 2022, *available at* https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/; Citizen Lab, "PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions," September 22, 2023, *available at* https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/.

[4] *See, e.g.*, Amnesty Tech, "Forensic Methodology Report: How to catch NSO Group's Pegasus," July 18, 2021, *available at* https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/; Amnesty Tech, "Dominican Republic: Pegasus spyware discovered on prominent journalist's phone," May 2, 2023, *available at* https://www.amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/; Amnesty Tech, "Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia," May 2, 2024, *available at* https://www.amnesty.org/en/latest/news/2024/05/unravelling-a-murky-network-of-spyware-exports-to-indonesia/.

[5] *See, e.g.,* Access Now, "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict," May 25, 2023, *available at* https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/; Access Now, "Hacking Meduza: Pegasus spyware used to target Putin's critic," September 13, 2023, *available at* https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/; Access Now, "New spyware attacks exposed: civil society targeted in Jordan," February 1, 2024; Access Now, "Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware," May 30, 2024, *available at* https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

Covenant on Civil and Political Rights, which the United States ratified in 1992 – protects individual rights to privacy, religious belief and conscience, opinion and expression. These rights are foundational to democratic societies, and spyware directly interferes with them. It causes individuals to doubt the privacy of their communications and opinions, strategically designed to cause people to question their intentions to engage in private and public discourse. Just days ago, one victim put the feeling this way:

> "The devastation I felt after discovering that the security agents who had tortured me in Bahrain had successfully hacked my phone and violated my privacy on British soil was overwhelming. I spent countless sleepless nights fearing the potential harm to those who had entrusted me with their sensitive information."[6]

As another put it, "'There were a lot of personal conversations which are not meant for anybody's ears. . . . For me, it was clearly a very dirty interference in my private life.'"[7] Galina Timchenko, co-founder, CEO, and publisher of the Russian-language media outlet Meduza, targeted with Pegasus spyware, said,

> "The only thing that I am really worried about is that those people whose devices were infected with Pegasus also sometimes became targets of physical attacks. So now I have to look over my shoulder. And if this was Russia, where any citizen can be persecuted for cooperating with 'undesirable organizations,' then my main fear is how can I protect other people, our partners? Because those who targeted me now have all of my contact list."[8]

The mere potential that spyware could be used against them causes victims – and would-be victims who do not know if they have been subjected to spyware – to question the safety of speaking their mind, risking a spiral of intimidation and self-censorship that eats at the foundations of democratic debate. I hardly need say this to legislators, but for democratic societies, that withdrawal can be fatal, particularly when the targets of such intrusions are those we depend upon to inform our public life and debate, such as human rights defenders, journalists and their sources, civil servants, and elected leaders like you.

As harmful as spyware is to human rights and democracy, evidence shows that spyware is also a national security threat. The Pegasus Project, a multinational journalistic reporting endeavor, suggested potential targets at the highest levels of democratic governments.[9] One investigative project reported that Vietnamese government agents sought to infect the phones of Members of Congress with Predator spyware, produced by the Intellexa Group, a group on the

---

[6] *See* Global Legal Action Network, "New Criminal Complaint Over Pegasus Spyware Hacking of journalists and activists in the UK", September 19, 2024, *available at* https://www.glanlaw.org/single-post/new-criminal-complaint-over-pegasus-spyware-hacking-of-journalists-and-activists-in-the-uk.

[7] Suzanne Smalley and Daryna Antoniuk, "The inside view of spyware's 'dirty interference,' from two recent Pegasus victims," THE RECORD, June 25, 2024, *available at* https://therecord.media/pegasus-spyware-victims-sannikov-erlikh.

[8] Natalia Krapiva, "Hacking Meduza: Pegasus spyware used to target Putin's critic, ACCESS NOW, September 13, 2023, *available at* https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/.

[9] *See, e.g.*, THE GUARDIAN, The Pegasus Project, *available at* https://www.theguardian.com/news/series/pegasus-project.

U.S. sanctioned entity list.[10] At the time that the Biden Administration announced its Executive Order addressing the spyware threat last year, it noted that "U.S. Government personnel overseas have been targeted by commercial spyware."[11]

The reporting from NGOs and journalists around the world indicated that one company, the Israel-based NSO Group, was responsible for many of the most egregious instances of spyware's abuse that have come to light. The NSO Group is part of a broader, opaque industry manufacturing, marketing, selling, transferring, and servicing mercenary spyware. The industry pitches its products as necessary for the control of terrorism and crime. Yet the industry has offered little proof of this claim of necessity, while the widespread exposure that commercial spyware has been used for state-on-state espionage belies the claims of necessity. On top of this lack of proof, there are troublingly few controls on the global proliferation and use of spyware. Even as the world became aware of the extraordinary abuses carried out using mercenary spyware, regulation and control, at national and international levels, lagged far behind.

In my 2019 UN report, I argued that it was imperative that governments limit the uses of spyware technologies to lawful ones only, subjected to the strictest sorts of oversight and authorization, and that they condition private sector participation in the spyware market – from research and development to marketing, sale, transfer and maintenance – on human rights due diligence and a track-record of compliance with human rights norms. I argued then that members of the industry should adopt and implement the UN Guiding Principles on Business and Human Rights, which establish a framework for companies to prevent or mitigate the human rights harms they cause,[12] but that responsibility, particularly in the context of such severe human rights impacts, must be overseen by public authorities and enforced by domestic and international law. At the time, I urged a moratorium on the industry, pending the imposition of enforceable rules, and while other UN rapporteurs and NGOs joined that call, civil society experts have developed a range of legal responses to spyware that include arguments for regulation and tighter export controls, while some even argue for a ban given the severity of the harms caused by spyware.

What is most remarkable, perhaps, apart from the persistent evidence of human rights and national security harms, is how quickly the industry rose and how rapidly its tools have been used against so many types of targets. Spyware's relative cheapness has enabled it to proliferate, destabilizing not only civil society but diplomatic and security sectors. It is easy to see how spyware's impact undermines fundamental democratic practice. But at the same time we are not safer when any government with access to spyware can hack, for instance, U.S. or NATO officials' phones. And yet this is the world to which we seem to be careening.

---

[10] Tim Starks, "The trail of Predator spyware leads to targets in Congress," THE WASHINGTON POST, October 10, 2023, *available at* https://www.washingtonpost.com/politics/2023/10/10/trail-predator-spyware-leads-targets-congress/.

[11] FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security, March 27, 2023, *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/.

[12] United Nations, GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS (2011), *available at* https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

One last point connects the spyware industry and the global threat landscape. The companies that make mercenary spyware often emphasize how much control they have over the technology when asked about proliferation risk. Yet recent work by Google's Threat Analysis Group has shown that Russian hackers obtained and used exploits, the building block of the spyware trade, previously used by NSO Group and Intellexa.[13] In this sense, the spyware industry is directly helping to fuel the capabilities of U.S. adversaries. The threats are that sophisticated, matching the persistence and intrusiveness typically only seen from states like Russia and China. This concerning nexus suggests that, at minimum, there is cross pollination between these industries, and that the mercenary spyware industry may be helping to buoy the exploit marketplace.

II. U.S. actions to address the spyware threat

The commercial spyware industry's intersecting threats to human rights and democracy and U.S. national security led the U.S. Government to act. In 2021, in the National Defense Authorization Act for 2022, Congress required the Secretary of State to prepare a list of contractors that have "knowingly assisted or facilitated a cyberattack or conducted surveillance" against the United States or against:

> ". . . [i]ndividuals, including activists, journalists, opposition politicians, or other individuals for the purposes of suppressing dissent or intimidating critics, on behalf of a country included in the annual country reports on human rights practices of the Department for systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights." 22 USC §2679e(a)(2).

In 2022, as part of the National Defense Authorization Act for 2023, Congress required U.S. intelligence agencies to provide annual reports assessing counter-intelligence threats "and other risks to national security" that "foreign commercial spyware" poses to the United States.[14] It further authorized the Director of National Intelligence to prohibit intelligence agencies from "entering into any contract or other agreement for any purpose with a company that has acquired, in whole or in part, any foreign commercial spyware."

The Biden administration, for its part, has taken steps to address the spyware problem consistent with U.S. law. In 2021, the Bureau of Industry and Security (BIS) of the Commerce Department added several companies, including the spyware companies NSO Group and Candiru, to the list of entities "engaging in activities that are contrary to the national security or foreign policy interests of the United States."[15] Specifically it noted,

---

[13] Google Threat Analysis Group, "State-backed attackers and commercial surveillance vendors repeatedly use the same exploits," August 29, 2024, *available at* https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/.

[14] Public Law 117-263 (50 USC §3232a) (2022).

[15] Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," November 3, 2021, *available at* https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

> "NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."[16]

In February of this year, BIS added Sandvine, a Canadian-incorporated company whose "technology has been misused to inject commercial spyware into the devices of perceived critics and dissidents."[17] In July of this year, BIS added four other entities to the Entity List for "trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide."[18]

The Department of Treasury's Office of Foreign Assets Control (OFAC) has identified several commercial spyware entities and persons associated with them as Specially Designated Nationals. As a result of such designations, all property and interests in property of such individuals or entities in the United States are blocked. Such spyware vendors as NSO Group and Intellexa have been designated under the program. For example, just this March, OFAC designated Intellexa and its key personnel "for their role in developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. government officials, journalists, and policy experts."[19]

In perhaps the most important example of the administration's recognition of the spyware threat to national security and foreign policy interests, in 2023 President Biden promulgated Executive Order 14093.[20] EO 14093 identifies a number of U.S. national interests, including the protection of "democracy, civil rights, and civil liberties." It condemns the use of commercial spyware to interfere with fundamental human rights, the rule of law and U.S. national security. As such, the order prohibits any federal agency or department from making operational use of commercial spyware when they determine *inter alia* "that the commercial spyware poses significant risks of improper use by a foreign government or foreign person."[21] The order further

---

[16] *Id.*

[17] Department of State, "The United States Adds Sandvine to the Entity List for Enabling Human Rights Abuses," February 28, 2024, *available at* https://www.state.gov/the-united-states-adds-sandvine-to-the-entity-list-for-enabling-human-rights-abuses/.

[18] Department of Commerce, "Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits," July 18, 2023, *available at* https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3297-2023-07-18-bis-press-package-spyware-document/file#:~:text=WASHINGTON%2C%20D.C.%20%E2%80%93%20Today%2C%20the,to%20gain%20access%20to%20information.

[19] U.S. Department of Treasury, "Press Release: Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium," March 5, 2024, available at https://home.treasury.gov/news/press-releases/jy2155.

[20] The White House, Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, March 27, 2023, *available at* 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/.

[21] EO 14093, Section 2(a).

articulates the bases upon which an agency could make such a determination, including uses in violation of international human rights law.[22]

In a demonstration of the emerging whole-of-government approach to spyware, moreover, acting under Section 212(a)(3)(C) of the Immigration and Nationalization Act, the Department of State established a program in February 2024 to restrict the issuance of visas to persons:

> "[b]elieved to have been involved in the misuse of commercial spyware, to target, arbitrarily or unlawfully surveil, harass, suppress, or intimidate individuals including journalists, activists, other persons perceived to be dissidents for their work, members of marginalized communities or vulnerable populations, or the family members of these targeted individuals".[23]

Importantly, the restrictions also apply to:

> "individuals believed to facilitate or derive financial benefit from the misuse of commercial spyware…including but not limited to developing, directing, or operationally controlling companies that furnish technologies such as commercial spyware to governments, or those acting on behalf of governments, that engage in [the misuse of commercial spyware]."

In addition to official steps by Congress and the Biden administration, individual litigants are seeking to use U.S. law in order to hold accountable spyware vendors and states that use spyware transnationally. A pending lawsuit brought by Meta (WhatsApp) against the NSO Group in U.S. courts may provide guidance as to the strength of various existing legal bases for remedy.[24] Yet barriers to accountability are real. In a case involving the Ethiopian government's hacking of an Ethiopian-American activist's computer in Maryland, a federal court ruled that the Foreign Sovereign Immunities Act (FSIA) barred the action, an indication that changes to the FSIA may be required to provide a further measure of action against those governments that use spyware as a tool of transnational repression.[25] Yet while these lawsuits are important examples of how cases may be brought, the global nature of the issue and jurisdictional hurdles make it hard for victims to hold companies accountable. This was the case, for instance, when the NSO

---

[22] *Id*., Section 2(a)(ii)(A)(1).
[23] Secretary of State Antony Blinken, "Press Statement: Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware," February 5, 2024, *available at* https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/.
[24] *See, e.g.*, Jonathon Penney and Bruce Schneier, "Platforms, Encryption and the CFAA: The Case of *WhatsApp v. NSO Group*," 36 Berkeley Tech. L. Journal 469 (2021), *available at* https://btlj.org/wp-content/uploads/2022/03/0005-36-1-Schneier.pdf.
[25] *See* Doe v. Federal Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017), *reh'g denied*, 2017 U.S. App. LEXIS 10084 (D.C. Cir. June 6, 2017).

Group's Pegasus spyware was used to hack journalists in El Salvador[26] (at least one of whom is a U.S. citizen[27]). Victims are seeking to hold NSO Group accountable in U.S. court.[28]

The United States is not alone among governments in having grave concerns about the commercial spyware threat. Poland has launched a major investigation into the previous government's use of Pegasus spyware against journalists and opposition figures, among others.[29] The European Parliament established a committee that, following extensive hearings, published a major report on the spyware threat in Europe, and the Parliament followed with several recommendations to European states.[30] Recognizing the global nature of the threat, and the resultant need for global solutions, the Biden administration has led a multilateral effort to counter spyware. In a Joint Statement issued on 30 March 2023, the United States and ten other States pledged to pursue "domestic and international controls" on spyware.[31] On the eve of this week's UN General Assembly, the State Department announced that additional states had joined the pledge, bringing to twenty-one the number of states signing up to counter spyware. That list now includes Australia, Austria, Canada, Costa Rica, Denmark, Estonia, Finland, France, Germany, Ireland, Japan, Lithuania, the Netherlands, New Zealand, Norway, Poland, Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States. The State Department is also setting aside funds to help low and middle income countries to develop better policies and oversight around spyware.[32]

These efforts may be having an impact on the spyware industry. Recently, the aforementioned Sandvine announced what appears to be a major transformation in its business, noting that, "In response to concerns regarding the misuse of our technology by foreign governments, we made a commitment to new ownership, leadership, and business strategy."[33] It has been suggested that, in light of the pressure from the United States and others, and the

---

[26] The Citizen Lab, "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," January 12, 2022, *available at* https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[27] Ronan Farrow, "A Hacked Newsroom Brings A Spyware Maker to U.S. Court," THE NEW YORKER, November 30, 2022, https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus.

[28] *See* Knight First Amendment Institute, *Dada v. NSO Group, available at* https://knightcolumbia.org/cases/dada-v-nso-group.

[29] Shaun Walker, "Poland launches inquiry into previous government's spyware use," THE GUARDIAN, April 1, 2024, *available at* https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

[30] *See* "European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware," *available at* https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html.

[31] U.S. Department of State, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," September 22, 2024, *available at* https://www.state.gov/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

[32] U.S. Department of State, "New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware," September 22, 2024, *available at* https://www.state.gov/new-u-s-led-actions-expand-global-commitments-to-counter-commercial-spyware/

[33] *See* Sandvine, "Our Next Chapter as a Market Leader for Technology Solutions," September 19, 2024, *available at* https://www.businesswire.com/news/home/20240919441171/en/Sandvine-Our-Next-Chapter-as-a-Market-Leader-for-Technology-Solutions.

recognition of investors that association with threats to democracy and national security are bad for business, the spyware industry faces serious threat.[34]

III. A Congressional Agenda to Counter Spyware

The spyware threat is potentially at an inflection point. The United States has taken firm action against the commercial spyware industry, and twenty-one governments have committed to taking robust actions to address the threat, but the evidence of continuing threat persists. The demand for spyware products remains, especially by governments that lack any kind of commitment to rule of law and the protection of fundamental human rights. AI tools are likely to infuse the spyware industry with an ever-deepening power to interfere with the foundations of democratic life and to expose U.S. and allied government officials and employees to the serious risks causes by targeted surveillance. All of this is happening at a time when U.S. adversaries like Russia and China are seeking to redefine what human rights in cyberspace even means – to eliminate the well-established principle that human rights offline apply online just the same.

This Subcommittee has the power to encourage the development of global norms to counter the spyware threat, to promote human rights and democracy and to protect U.S. interests and national security. The Joint Statement on countering commercial spyware, mentioned above, contains a set of global commitments which Congress should support. A Congressional agenda should include the following:

1. Congress could ensure that the rules of Executive Order 14093 are codified as statutory obligations of U.S. agencies. But it could also go beyond EO 14093. For instance, as noted above, victims face serious barriers when they seek to hold foreign states accountable for hacking that implicates them in the United States. Federal courts, for one thing, have adopted a narrow reading of the Foreign Sovereign Immunities Act. Congress could explore ways to make remedies available to such victims in U.S. courts.[35]

2. Congress could encourage other governments to join the global effort to constrain commercial spyware. Congressional support for EO 14093 would go a long way in this direction. But in the face of the increasing threat of spyware's proliferation, Congress could also adopt appropriate conditions on U.S. assistance to or cooperation with other governments on their commitments to prevent, consistent with the 2023 Joint Statement, the export of software, technology, and equipment to end-users likely to use them for malicious cyber activity; it could condition assistance to other governments on their commitment to adopt, implement and demonstrate, at a minimum, that rule of law and human rights standards apply to their use of commercial spyware technologies.

---

[34] See Omer Kabir, "Is Israeli spyware a dying sector?" CALCALIST, April 23, 2023, *available at* https://www.calcalistech.com/ctechnews/article/twcgg3tql.

[35] *See* Spencer Levitt and Andrea Cervantes, *The Foreign Sovereign Immunities Act in the Age of Transnational Surveillance: Judicial Interpretation and Legislative Solutions*, Report of the UC Irvine School of Law International Justice Clinic, August 21, 2023, *available at* https://bpb-us-e2.wpmucdn.com/sites.uci.edu/dist/2/4290/files/2023/08/The-Foreign-Sovereign-Immunities-Act-in-the-Age-of-Transnational-Surveillance.pdf.

3. In keeping with the 2023 Joint Statement, Congress could also ensure that civil society groups have a place at the table in the national and global efforts to counter commercial spyware. It has been civil society organizations, after all, that have led the way in exposing the global threat of the commercial spyware industry. Further hearings like this one should bring the voices of security researchers, victims and their advocates to public awareness.

4. Congress could reinforce administration efforts to engage additional partner governments around the world to mitigate the misuse of commercial spyware and drive reform in this industry, including by encouraging industry and investment firms to implement the United Nations Guiding Principles on Business and Human Rights. A range of regulatory measures are available, drawing on experiences in other areas of international law, and Congress could play a meaningful role in pressing forward these ideas.[36]

In addition to spyware-specific steps, the Congressional voice could have near-term impact in a related area. This Fall, the UN General Assembly is considering adoption of a new Cybercrime Convention. The draft Convention, originally an initiative pressed by the Russian Federation, may on its face appear to be a salutary effort to promote international cooperation. But its loose language and broad framing of "serious crimes" opens the door to a confusing international legal landscape that will almost certainly work to the detriment of human rights. The Freedom Online Coalition Advisory Network has called the draft "a far-reaching global criminal justice treaty that would enable and legitimize serious human rights violations due to multiple flaws and lack of safeguards and fundamental rights protections."[37] It has the potential to, at the very minimum, send a contrary message on government targeted surveillance at the very moment that the United States is pushing for constraint.[38] In advance of the UN General Assembly vote on the draft, Senate expressions of concern could focus U.S. Government and allied attention on the potential harm the convention could do and urge them to reject it.

In this way, my testimony returns to the beginning. Commercial mercenary spyware poses serious threats to cyberspace – but more specifically, to human rights and national security. It has become one of the key vectors for the furtherance of authoritarianism and repression in the digital age. But democracies need not be sitting ducks; they have the tools to counter the rise of global authoritarianism in cyberspace. The United States has begun to deploy rule of law in the face of spyware's lawlessness, and I urge the Subcommittee to continue its critical support of the legal fight for freedom online.

---

[36] *See, e.g.*, David Kaye and Sarah McKune, "The Scourge of Commercial Spyware – and How to Stop It," LAWFARE, August 25, 2023, *available at* https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it.

[37] FOC Advisory Network Proactive Advice: UN Convention Against Cybercrime, September 16, 2024, *available at* https://freedomonlinecoalition.com/foc-advisory-network-proactive-advice-un-convention-against-cybercrime/.

[38] *See* Kate Robertson, "A Global Treaty to Fight Cybercrime – Without Combating Mercenary Spyware," LAWFARE, August 22, 2024, *available at* https://www.lawfaremedia.org/article/a-global-treaty-to-fight-cybercrime-without-combating-mercenary-spyware.