Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the United Nations Working Group on the Use of Mercenaries

March 25, 2026

Report authors:

Ronald Deibert
Sarah McKune

For all inquiries regarding this submission, please contact:

Dr. Ronald J. Deibert, Director, The Citizen Lab, Munk School of Global Affairs, Professor of Political Science, University of Toronto, r.deibert@utoronto.ca

This submission is to provide input from the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, in response to your call for inputs regarding the use of technology in the operations and activities of mercenaries, mercenary-related actors and private military and security companies. In particular, this letter highlights for your attention key legal and policy issues concerning state reliance on the private sector in digital operations undertaken for national security, law enforcement, or intelligence purposes. These are the issues that, based on Citizen Lab research as well as the work of numerous other civil society groups and journalists over many years, remain significant obstacles to ensuring compliance with international human rights law by states and the private sector. The attention and guidance of the Working Group on these issues in its forthcoming report will be of great importance given the expanding privatization of state action in these fields.

Increasing Privatization of State Security Functions

For many years the Citizen Lab has researched and analyzed the use of mercenary spyware against civil society and other actors. We have documented incidents of misuse and raised concerns about the human rights impacts of such technology in a number of reports. While some progress has been made at the international level with respect to development of norms and regulations that would constrain misuse of digital surveillance tools, recent trends suggest serious potential for backsliding and entrenchment of impunity in the space. As states increasingly integrate private sector providers of advanced digital technologies including spyware in their security apparatus, they have failed to ensure that mechanisms for oversight, accountability, and transparency in line with international human rights law keep pace.

Recent shifts in the US have the potential to accelerate growth within the market for advanced digital technologies with national security, law enforcement, or intelligence applications, while degrading legal and policy restraints preventing misuse. The US administration has signaled its intent to work closely with and rely upon the private sector in the conduct of critical state operations, including with respect to national security, offensive cyber, and immigration enforcement, drawing on AI, facial recognition, and other surveillance and analysis tools. At the policy level, the US National Security Strategy (November 2025) highlights the importance of the private sector to the administration's strategic interests in the digital environment, and flags deregulation as a priority:

> [T]he U.S. Government's critical relationships with the American private sector help maintain surveillance of persistent threats to U.S. networks, including critical infrastructure. This in turn enables the U.S. Government's ability to conduct real-time discovery, attribution, and response (i.e., network defense and offensive cyber operations) while protecting the competitiveness of the U.S. economy and bolstering the resilience of the American technology sector. Improving these capabilities will also require considerable deregulation to further

> improve our competitiveness, spur innovation, and increase access to America's natural resources.

The US Cyber Strategy (March 2026) elaborates further:

> We will outcompete adversaries who sell "low cost" AI and digital technologies that carry embedded censorship, surveillance, and ideological bias. We will partner closely with industry and academia, at the speed and scale commensurate with the threats we face, and in accordance with our values. . . . [W]e will dismantle networks, pursue hackers and spies, and sanction lawless foreign hacking companies. We will unveil and embarrass online espionage, destructive propaganda and influence operations, and cultural subversion.
>
> By disrupting adversaries' cyber campaigns, and making our networks more defensible and resilient, we will unleash innovation, accelerate economic growth, and secure American technology dominance. We will remove burdensome, ineffective regulations so that our industry partners innovate quickly in emerging technologies. Partners in the private sector must be able to respond and recover quickly to ensure continuity of the American economy. . . . We will leverage the immense talents and ingenuity of our private sector research base. We will establish a new level of relationship between the public and private sectors to defend America in peace and war.

In effect, the US administration has linked its national security imperatives with the growth of American industry, prioritizing the participation of and potential benefits to the private sector in its security policies while loosening regulatory control. At present this approach is most visible within the US immigration enforcement apparatus, including CBP and ICE, which have rapidly incorporated a wide array of digital technologies and services provided by the private sector. At the same time, the US administration has downsized the federal workforce traditionally responsible for offensive and defensive cyber operations, including at the National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA), leaving gaps that it may seek to address through private contracts.

The foreseeable result is a privatized system that relies on state revenue and accelerated growth through state contracts, yet introduces even more hurdles to achieving public transparency, oversight, and accountability in these sensitive spaces. The potential for abuse and impunity is vast, with reports already emerging of the outsize influence of private sector actors, such as Palantir and its executives, on global public policy. Indeed, the US administration, in line with its 2025 AI Action Plan that emphasizes deregulation of AI and its use in warfighting, has already taken punitive measures against AI company Anthropic to eliminate application of company-specified safeguards to use of its

technology by the "Department of War." Should the US become a jurisdictional haven for deregulation, investment, and private sector growth outside the bounds of corporate social responsibility, we can expect to see even more extensive human rights abuses associated with the market for advanced digital technologies.

Key Legal and Policy Issues of Concern

A number of challenges exist within this landscape to ensuring human rights compliance by states and the private sector, which may inform the Working Group's consideration of recommendations for its forthcoming report. These challenges include:

1. **Determining the appropriate scope of the concepts of "inherent state function" and "prohibited activities" in the context of advanced digital technologies with security applications provided by the private sector.**

As the Working Group has elaborated, certain activities that implicate the state monopoly on legitimate use of force constitute inherent state functions, the outsourcing of which "creates risks for the violation of human rights, including obstacles to accountability and remedy for victims of human rights violations." According to the Working Group, "States must be particularly vigilant when they outsource inherent government functions to private commercial actors that are motivated primarily by profit, fostering situations in which human rights are subordinated to goals of efficiency, effectiveness and cost-cutting." Likewise, the Open-Ended Intergovernmental Working Group to elaborate the content of an international regulatory framework relating to the activities of PMSCs envisions a set of "prohibited activities" that States "cannot outsource" to PMSCs "under any circumstance," which include participation in acts of aggression or other activities prohibited under the UN Charter.

With states such as the US signaling their intent to privatize a wide array of digital operations critical to law enforcement, intelligence, and national security, further guidance from the Working Group on the scope of digital activities over which states must maintain a high level of control and oversight, or prohibit outsourcing in the first instance, will be particularly important. Indeed, the risk to human rights and stability in the digital ecosystem at large is exemplified in proposals that states deputize the private sector to "hack back" – engage in offensive cyber operations – which the Working Group has previously flagged as an area of concern. The concept of inherent state function or prohibited activities should specifically address the modern surveillance climate and the "authoritarian stack," which clarification may facilitate multistakeholder discussions regarding the level of control that should remain in the hands of the state in order to ensure that the use cases and implementation of such technologies serve the interests of the public rather than the private sector.

2. **Unique attributes of the mercenary spyware trade that may confound application of human rights and other legal frameworks, and present significant sectoral risk.**

Addressing the human rights impacts of the mercenary spyware sector in particular will require a tailored approach that factors in the following key attributes of the sector:

a. The mercenary spyware trade is built on secrecy.

All aspects of the mercenary spyware trade serve the goal of maintaining secrecy of operation. Client states demand secrecy from spyware companies when purchasing and using the tool, including through contractual commitments, ostensibly to protect national security or law enforcement interests. Companies rely on such state secrecy to avoid reputational impact or legal action while proliferating products and services. Host states shelter the spyware companies in their jurisdiction through favorable regulatory environments, including limitations on transparency in export licensing. Shifting the design and servicing of commercial cyber intrusion to the private sector enables another layer of corporate secrecy, not least of which is the ability to hide investment and ownership through offshore services and corporate shells. And the technology itself is designed for covert installation and operation while eliminating traces of its presence on a device. Unlike traditional private military and security companies operating in the field, there is no way to physically observe the mercenary spyware trade in action, and very few means of obtaining information, significantly complicating oversight.

It is difficult to envision a multistakeholder framework, akin to the International Code of Conduct Association (ICoCA) built around the Montreux Document, that could effectively function in this space, given its endemic secrecy. Transparency is the critical missing component, as to clients, companies, supply chains, and investors. A new understanding of what transparency and accountability in this space could look like is needed.

Working Group guidance on such questions could include recommendations for effective parameters regarding transparency, heightened scrutiny, and oversight of the sector, drawing on the Global Principles on National Security and the Right to Information (the Tshwane Principles), the Venice Commission's 2024 Report on a Rule of Law and Human Rights Compliant Regulation of Spyware, and Inter-American jurisprudence, recently explored in the 2025 report regarding digital surveillance prepared by the Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR).

b. Growth in the mercenary spyware trade depends on increasing demand by states for its products and services, which runs counter to principles of international human rights law that require invasive state surveillance to be *exceptional*.

As is well-established in international human rights law, any use of surveillance technology that restricts the rights to freedom of expression and privacy is exceptional, permissible only when in furtherance of a legitimate aim recognized under human rights law and in accordance with the principles of legality, necessity and proportionality. Restrictions "may not put in jeopardy the right itself... [T]he relation between right and restriction and between norm and exception must not be reversed." Yet the expanding mercenary spyware trade and its rapidly developing capabilities have the effect of normalizing such surveillance operations. It would be beneficial to mutlistakeholder discussion for the Working Group to address this tension at the heart of the mercenary spyware question: on what basis can the growth-oriented private sector participate in operations that legal frameworks require states to minimize? For example, the Working Group could consider whether states and/or companies should deploy additional guardrails around private investment in mercenary spyware companies, or restrict the number of active licenses available to client states.

c. The mercenary spyware trade capitalizes on – and states that rely on the trade incentivize – innovation that undermines the security of the digital ecosystem at large, the costs of which are borne by targeted platforms and compromised users.

The mercenary spyware trade presents significant sectoral risk, in that its business model is structured on developing, servicing, and maintaining access to digital exploits that rely on security vulnerabilities in consumer-facing digital platforms, all while companies assert that they have little oversight of their technologies after providing them to clients (which assertion has in some cases proven inaccurate). At present the negative externalities associated with the trade are largely borne by targeted platforms and users. While some have engaged in legal action against spyware companies and state actors, numerous hurdles exist to seeking and obtaining remedy. As noted in the 2025 report regarding digital surveillance prepared by the Special Rapporteurship for Freedom of Expression of the IACHR, the impunity that characterizes this space ultimately results in a state of continuous violation of the rights of individuals targeted, because perpetrators and enablers of intrusive digital surveillance refuse to divulge information regarding the fact or scope of surveillance, or provide guarantees of non-repetition.

The Working Group may wish to provide guidance on how to properly allocate the risks associated with the mercenary spyware trade, in a manner that effectuates access to remedy and ensures that the entities benefiting from the trade likewise assume the significant costs. This is an issue area that is relatively under-explored in multistakeholder debate. For example, potential levers available to host states to shift risk and formalize transparency and reporting requirements could include restrictions on government loans, contracts, and collaboration, or other government investment, as well as tax penalties, for companies implicated in misuse; sectoral insurance requirements with independent

channels for incident claims; or legislation mandating vulnerability disclosure in accordance with accepted standards when misuse is established, or at designated points within the lifecycle of the technology.

3. **Potential for corruption.**

As documented by civil society, experts, and journalists, mercenary spyware companies, as well as other high-profile private sector entities providing or investing in advanced digital security technologies, often enjoy close ties to government officials and establishments. Companies active in the space frequently employ leadership or expertise that comes out of government agencies, or utilize significant company resources to hire well-connected lobbyists, PR firms, and other advocates. At the same time, these entities typically operate under the cover of state secrecy, and provide tools designed to compromise sensitive information, as explained above. Spyware in particular has been used in many instances by government officials for political advantage. Such conditions, which appear poised to intensify, heighten the risks of corruption and discriminatory dealing in this sector.

The issue of corruption has not yet been fully addressed in multistakeholder discussion regarding the use of spyware and other surveillance and intrusion tools, but given current trends and developments, it is apparent that the topic is ripe for consideration. The Working Group may wish to consider the relevance of the UN Convention Against Corruption, and Section VII of the OECD Guidelines for Multinational Enterprises for Responsible Business Conduct, in assessing legal frameworks applicable to state authorities' potential reliance on the private sector in utilizing digital technologies for purposes of undue advantage.

4. **Potential for contravention of the principle of non-discrimination.**

In the mercenary spyware context, it has come to light that private sector companies may design and implement their technologies to prevent installation of spyware on devices bearing indicators of specific national origin. For example, in the case of NSO Group, the company has claimed that their technology is technically prevented from operating on devices with US-based mobile phone numbers, while other reports suggest that Israel- or "Five Eyes"-based phone numbers are protected, presumably because those jurisdictions hold significant sway over the company's commercial strategy and success. It is unclear whether this approach is standard industry practice, but given the prevalence of misuse of such tools, it is highly plausible that host states, client states, or companies themselves insist on geolimitations within the technical design and implementation of intrusion tools.

Such design and implementation practices raise the question of whether the mercenary spyware trade runs afoul of the principle of non-discrimination, as provided for in Article 2, paragraph 1 of the

International Covenant on Civil and Political Rights (ICCPR). As the UN Human Rights Committee has explained, states party to the ICCPR are "responsible for ensuring the equal enjoyment of rights without any discrimination. Articles 2 and 3 mandate States parties to take all steps necessary . . . to put an end to discriminatory actions both in the public and the private sector which impair the equal enjoyment of rights." The Committee, in its General Comment No. 18, interpreted the term discrimination to mean "any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms." Mercenary spyware that categorizes individuals by indicators of national origin in order to greenlight an infection, thereby violating a host of human rights, is *prima facie* discriminatory exposure. The Committee has emphasized in General Comment No. 31 that States Parties must also ensure that private sector entities do not engage in discriminatory action: "There may be circumstances in which a failure to ensure Covenant rights" – including, the Committee noted, the right to privacy – "as required by article 2 would give rise to violations by States Parties of those rights, as a result of States Parties' permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities."

Indeed, the existence of geolimitation features within mercenary spyware is a tacit admission that misuse is an anticipated collateral feature of the spyware trade, with geolimitation designed to curtail negative impacts upon and/or reduce risk with respect to a preferred subset of potential targets. The rationale for such differentiation in treatment may be to ensure continued access to markets and prevention of misuse in a manner that undermines the company's commercial interests or the geopolitical interests of a host state; anyone of a national origin that is considered of insufficient global stature, however, may still be targeted. It is possible that similar technical parameters could be applied within other digital surveillance or analysis tools as well. Guidance on the question of non-discrimination in the context of mercenary spyware may thus help inform the design and use of highly invasive technologies more broadly.

We at Citizen Lab are available for further discussion or inquiry as the Working Group prepares its report. Thank you for your attention to these important issues.