UNITED STATES MISSION TO THE UNITED NATIONS
NEW YORK

POL 2025-04-corr.

The United States Mission to the United Nations presents its compliments to the Permanent Missions and Observer Offices to the United Nations and has the honor to circulate an updated concept note to Permanent Representatives and Permanent Observers regarding the Arria-formula meeting on “Commercial Spyware and the Maintenance of International Peace and Security.”

The Arria-formula meeting is co-sponsored by the Permanent Missions of Australia, Austria, Canada, Estonia, Finland, France, Japan, Latvia, Lithuania, the Netherlands, Norway, Poland, the Republic of Korea, Sweden, and the United Kingdom to the United Nations.

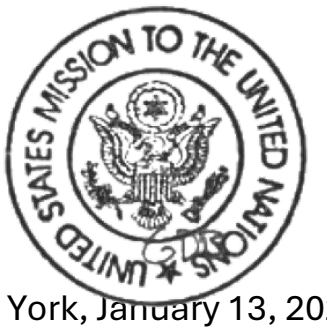
The meeting will take place on Tuesday, January 14, from 3:00-6:00 p.m. in the ECOSOC Chamber at the United Nations Headquarters Building.

Permanent Missions and Observer Offices
to the United Nations
New York

DIPLOMATIC NOTE

The United States Mission to the United Nations avails itself of this opportunity to renew to all Permanent Missions and Observer Offices to the United Nations the assurances of its highest consideration.

Enclosure: As stated.



New York, January 13, 2025

CONCEPT NOTE:
Arria Formula Meeting on
Commercial Spyware and the Maintenance of International Peace and Security
Tuesday, January 14, 2025, 3:00-6:00pm
ECOSOC Chamber

Overview: On Tuesday, January 14, at 3:00 pm, the United States, with the co-sponsorship of Australia, Austria, Canada, Estonia, Finland, France, Japan, Latvia, Lithuania, the Netherlands, Norway, Poland, the Republic of Korea, Sweden, and the United Kingdom will convene an Arria-formula meeting of the UN Security Council to address the implications of the proliferation and misuse of commercial spyware for the maintenance of international peace and security. Member States are invited to learn about this novel new threat and discuss the way forward for efforts to mitigate the risks associated with the deployment of commercial spyware in the peace and security context.

Strengthening Global Awareness of the Spyware Threat: There is growing international attention to the acute threat posed by the misuse of commercial spyware and the need for strict controls on the proliferation and use of such technology. Public reports have shined a bright light on the robust market for powerful spying tools that are sold on the open market. The most sophisticated of these tools provide "zero click" access to all the information stored on a mobile phones, laptops, or other internet-connected devices. E-mails, photographs, messages sent via encrypted apps, even the microphone on a device — nothing is out of reach. This spyware has proven to be a game changer for governments looking for new means to surveil, intimidate, imprison, track, or target individuals without proper legal authorization, safeguards, or oversight.

States are increasingly committing to taking joint action through which to address this shared threat, including through the 2023 Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, and 2024 Pall Mall Process on tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. In October 2024, during the 57th session of the Human Rights Council, Member States agreed to language recognizing the threat commercial spyware misuse poses to democratic values and the exercise of human rights and fundamental freedoms. Adoption of this language by consensus of all member states of the UN Human Rights Council built on the 2023 Joint Statement in the Human Rights Council signed by 59 countries affirming that surveillance technologies, including commercial spyware, must not enhance the capacity of governments to violate human rights. The adoption of this landmark language followed a September 2024 meeting that the United States convened on the margins of the UN General Assembly. During that session, representatives from nearly two-dozen Member States underscored their commitment to stand with the victims of human rights abuses, establish guardrails on this technology, and hold those who misuse it accountable.

Implications for International Peace and Security: The misuse of commercial spyware presents significant and acute risks to international security, including to the safety and security of both government and UN personnel, as well as information systems. During the 79th Session of the UN General Assembly, Member States expressed concern that the dissemination of Information and Communications Technologies (ICT) intrusion capabilities by State and non-State actors could contribute to unintentional escalation and threaten international peace and security. For example, independent researchers announced in May 2023 that public figures and officials, including journalists and human rights defenders, were targeted with spyware amid conflict in Nagorno-Karabakh, during the period October 2020 and December 2022. Separately, the Rapid Support Forces, a paramilitary group in Sudan accused of committing crimes against humanity, reportedly imported commercial spyware for use in its ongoing conflict against the Sudanese government, a war that has created the worst humanitarian crisis in the world. Yet other reports confirmed the use of commercial spyware against individuals in areas and conflicts with peacekeeping missions authorized by the United Nations Security Council.

Topics for Discussion: This Arria-formula meeting aims to build on discussions between Member States and to advance global dialogue on the commercial spyware challenge, including by addressing the following questions:

- How could member states govern the proliferation and use of commercial spyware, so as to contribute and not undermine international peace and security?
- What additional steps can Member States take to discourage investment in and the export of commercial spyware products that are routinely misused in ways that undermine international peace and security, as well as fundamental human rights?
- What steps can Member States take to ensure appropriate safeguards are implemented to mitigate potential risks associated with the use of commercial spyware in conflicts?

Briefers:

- **John-Scott Railton**, Senior Researcher, Citizen Lab at the University of Toronto
- **Shane Huntley**, Senior Director, Google Threat Intelligence Group
- **Julia Gavarrete**, Salvadoran journalist specializing in political issues, migration and human rights