United States Senate
WASHINGTON, DC 20510

September 19, 2024

The Honorable Secretary Antony Blinken
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, D.C. 20520

Dear Secretary Blinken,

We write to request information from the Department of State regarding the international deployment of artificial intelligence (AI), particularly in conflict settings.

We commend the Department of State's release of the *United States International Cyberspace & Digital Policy Strategy*, which recognizes that repressive regimes and other actors "have used cyber and digital tools to threaten international peace and stability, harm others, exert malign influence, and undermine human rights." [1] Like the Department, we believe that the innovative use of cyber and digital tools—including AI—must be grounded in human rights and appreciate the *Strategy*'s emphasis on international cooperation toward this goal. The *Strategy* is more important today than ever, given the rapid development of AI capabilities and the technology's increasing integration into critical systems—including weapons and targeting systems, as exemplified by the current Israel-Hamas war. [2]

We also want to acknowledge the Department's role in supporting the U.S.-led *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy* and commend the development of international norms for responsible use of AI in armed conflict. [3] The endorsement of the declaration by 45 countries illustrates the importance of the declaration; it also highlights the seriousness of countries that have *not* endorsed the *Declaration*, including Israel.

Finally, we are encouraged by the recent release of the *Risk Management Profile for Artificial Intelligence and Human Rights*. [4] The development of a practical guide for organizations and governments to govern, map, measure, and manage AI derived human rights risks is a critical first step in protecting vulnerable populations. We urge the Department to consider how to apply

---

[1] United States Department of State, *United States International Cyberspace & Digital Policy Strategy,* https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/#threats.

[2] Sophia Goodfriend, "Why human agency is still central to Israel's AI-powered warfare," *+972 Magazine*, April 25, 2024, https://www.972mag.com/israel-gaza-lavender-ai-human-agency/.

[3] United States Department of State, *Political Declaration on Responsible Use of Artificial Intelligence and Autonomy,* https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-3/

[4] United States Department of State, *Risk Management Profile for Artificial Intelligence and Human Rights,* https://www.state.gov/risk-management-profile-for-ai-and-human-rights/.

the existing *Profile* and expand it, as necessary, to fully evaluate potential human rights violations in conflict settings.

To better understand the Department's ongoing efforts in support of the *Strategy,* the *Declaration*, the *Profile*, and any other relevant initiatives, we request the following information regarding foreign countries' use of AI technologies, no later than October 21, 2024. The information provided should be unclassified to the greatest extent possible, though may include a classified annex:
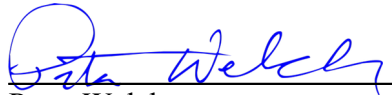
1. From the Department's perspective, what critical and emerging AI technologies are most meaningfully and significantly impacting military capabilities and diplomatic relationships? Which countries are most advanced in the development and adoption of these technologies, and what are some examples of such technologies of concern?

2. In cases when an emerging AI technology has been deployed in an armed conflict and civilians' rights and safety appear to be at higher risk, how much is attributable to the nature of the technology, the technology's reliability, or the absence of clear policies and protocols to reduce such risks?

3. Where is there strong global alignment with the *U.S. International Cyberspace and Digital Policy Strategy*? Where is there weak global alignment? What are the proposed recommendations to improve digital solidarity, specifically around ethical AI deployment?

4. Whether through the previously discussed pathways – like the *International Cyberspace and Digital Policy Strategy*, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, or *Risk Management Profile for Artificial Intelligence and Human* Rights – or other initiatives, what are your next steps for evaluating the deployment of AI in armed conflict and ensuring civilian harms are minimized?

5. The Department currently releases Country Reports on Human Rights assessing the human rights practices of countries receiving U.S. assistance, among other reports.[5]

   a. In which existing Department of State reports, such as human rights reports, could the Department include information regarding foreign countries' use of cyber and digital tools? What benefit, if any, does the Department see in incorporating this information?

   b. How would an annual report to Congress that outlines the cyber and digital technology capabilities of foreign countries help Congress support the Department's work to implement the *Strategy* and promote compliance with international humanitarian law*?*

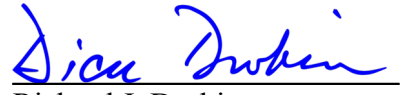[5] United States Department of State, "2023 Country Reports on Human Rights Practices," April 22, 2024, https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/.

We urge the Department of State to proactively and publicly engage in setting international norms regarding the ethical deployment of AI technology. We look forward to working with you to help ensure a rights-respecting digital future.

Sincerely,

Peter Welch
United States Senator

Richard J. Durbin
United States Senator