THE DOSSIER

Women, Peace, and Cybersecurity

By Diana Park and Kinsey Spears

Executive Summary

Since the Women, Peace, and Security (WPS) agenda entered the discussion among policymakers three decades ago, the security environment has been transformed, in part due to innovations in information and communications technology (ICT). As the cyber policy community grapples with the implications of cyberspace, a uniquely human-constructed domain of warfare, there is ample opportunity for WPS engagement in these issues. Discussions have yet to evolve and expand around gender and cyberspace operations.

The U.S. 2019 WPS Strategy does not recognize outright the importance of integrating the cyber and WPS agendas into one coherent effort. It does, however, lay out a framework to illustrate how these two policy communities can begin a dialogue around common objectives. This report addresses this incongruence using the objectives laid out in the 2019 WPS strategy.

Key Takeaways

- Marginalized groups, particularly girls and women, have less access to technology than boys and men. The gender gap in the broader cyber workforce has further implications for how technology itself continues to perpetuate gender-based bias, including in artificial intelligence and machine learning.

Palestinian female students attend the Arduino Applications training at Spark for Innovation and Creativity in Gaza City on February 28, 2023. (Photo by Majdi Fathi/NurPhoto via Getty Images)

- Gender amplifies the human security implications of cyberspace, such as digital privacy, radicalization, harassment, gendered disinformation, or abuse that occur virtually, as well as physical violence that is directly impacted by policies and actions in cyberspace.

- There have been some calls for action from national and international actors on improving the integration of cybersecurity into the WPS agenda and vice versa. However, globally there is limited traction on incorporating cybersecurity and cyber threats into WPS National Action Plans or bringing WPS into relevant cybersecurity policies and initiatives.

Policy Recommendations

1. The National Strategy for Women, Peace, and Security, which is currently being updated and revised, must include cyber considerations. Each implementing agency (the U.S. departments of State, Homeland Security, and Defense, as well as the U.S. Agency for International Development) should include actionable changes on WPS and cybersecurity in their agency-specific implementation plans.

2. The WPS and cybersecurity agenda must more robustly include cybersecurity, and the White House and the U.S. government's cybersecurity community need to be more active in incorporating WPS and gender analysis into their strategies.

3. Increase hiring for WPS and cybersecurity experts, including at the Office of the National Cyber Director and The Cybersecurity and Infrastructure Security Agency.

4. The U.S. needs to work with its allies and partners to incorporate WPS considerations into *all* cybersecurity measures at the United Nations.

5. The Biden administration needs to take an aggressive approach to tackling data privacy, especially given evolving threats to data and privacy protections on reproduction and sexual health information across the country.

6. The WPS community should play a leading role in investigating the overlap between gender and atrocity prevention in cyberspace. With a more robust understanding of the ways that gender-based harassment and threats play out online, the WPS agenda should engage more fully with its cyber policy counterparts to explore how technology can play a role in early warning and prevention.