Mavic Cabrera-Balleza’s speech at the International Day for the Elimination of Sexual Violence in Conflict. 19 June 2023. UN HQ, New York

Good morning! Thank you for the opportunity to speak with all of you today as we mark the 9th official observance of the International Day for the Elimination of Sexual Violence in Conflict.

Thanks to the Offices of the SRSG on Sexual Violence in Conflict, and for Children and Armed Conflict, and the Permanent Mission of Argentina to the United Nations for co-hosting this essential conversation on “Bridging the gender digital divide to prevent, and address conflict-related sexual violence.”

This event is critically important as our digital and real worlds have merged and shaped each other. Nowadays, digital technologies such as data pooling and Artificial Intelligence are used regularly to monitor and assess trends in health, education, environment, finance or perform daily tasks such as navigating traffic or paying a bill.¹

The use of AI in conflicts has also become increasingly apparent. In the raging war in Ukraine, the proliferation of weapons systems is aided by AI.²

As to social media, in 2023, an estimated 4.9 billion people use social media across the world.³ Digital technologies enable people to make their voices heard and to talk to people around the globe in real time. These spaces are critical in conflicts and during global crises such as the COVID-19 pandemic. At the Security Council briefing on ICTs in May 2022, Rosemary DiCarlo, UN Under-Secretary-General for Political and Peacebuilding Affairs, highlighted that “The benefits of digital technologies for maintaining international peace and security are manifold. In Yemen, the United Nations Mission to Support the Hudaydah Agreement has used mapping, geographic information systems, and satellite tools to enhance its monitoring of the ceasefire, Under Secretary DiCarlo also cited the United Nations Support Mission in Libya (UNSMIL) that has held five digital dialogues — each involving more than 1,000 participants — increasing the legitimacy of a process that enabled communities to get their voices heard.⁴ Online platforms are also effective in disseminating information on specialized assistance, including a toll-free hotline for survivors of sexual violence.

However, it can also reinforce prejudices and sow discord by giving hate speech, misinformation, and disinformation on several wide-reaching platforms. As such, social media algorithms fuel the fragmentation of societies and communities. They expand the reach of sex trafficking and pornography and facilitate gender-based violence.

---

¹ Mavic Cabrera Balleza is the Founder and CEO of the Global Network of Women Peacebuilders
In South Sudan, and Yemen, despite some gains in their participation in peace processes, it is the women peacebuilders who are threatened and discredited in social media and sent threatening messages on their cell phones. In the Philippines, women political dissenters and their female family members are threatened with rape.

Despite the documented cyber insecurity, compounded by women’s lack of access, and limited knowledge to navigate cyberspace, the lack of adequate response from telecommunication companies as well as Member States is deeply concerning. Most national cybersecurity policies that could have been instruments in addressing technology-facilitated GBV do not address these issues! From our research at the Global Network of Women Peacebuilders supported by Switzerland, we learned that there are 120 national cybersecurity strategies, certainly more than the 107 NAPs on WPS. Most national cybersecurity strategies do not have a gender perspective and are entirely detached from NAPs on WPS. Many national cybersecurity strategies do not involve CSOs in their development and implementation.

A more complex problem in cybersecurity interventions is when the State misuses cyber security policies for political purposes and becomes a cyber threat actor. For example, by silencing political opponents through censoring online content, spreading online propaganda, using surveillance technologies against civil society and other dissenters, or using the fight against disinformation as a pretext for prosecution.

Member States, the UN, civil society, research and educational institutions, and the ICT sector must turn the double-edged character of digital technologies into an opportunity to build consensus on how the technologies can be used for the good of people and the world while addressing the risks they present. Here are my recommendations on how we can do this:

1. Member States must work with civil society to ensure that digital technologies are accessible to all, culturally sensitive, and that the internet is a safe and empowering space for women and girls.

2. Member States must fully and equally involve civil society in developing and implementing national cybersecurity strategies. Such strategies must take a whole of nation approach and integrate a Women, Peace, and Security perspective. Cybersecurity does not have to come at the expense of women’s rights and democracy.

3. Diverse women must be encouraged and supported to enter the digital technology profession and lead research and development to prevent the misuse of digital platforms. Women remain underrepresented in tech. According to GovTech Singapore, women make up only a little under 30% of the tech workforce globally. This gap further aggravates gender disparities across other sectors.

4. Telecommunication companies must not be allowed to amass profit while their platforms continue to be the site of online sexual and gender-based violence. They must be held accountable for monitoring online content and not allow them to solely decide what is acceptable online. What is acceptable should be in line with international standards for peace.

---

519 in Africa; 18 in the Americas; 13 in Arab States; 23 in Asia and the Pacific; 6 in CIS; 41 in Europe. Accessed from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
and security, human rights and sustainable development, and feminist principles.

Now, more than ever, we need to understand the connections between gender and cybersecurity and recognize the need to protect women’s rights, human rights, and human security in cyberspace. Only then can we develop crucial policies to address cyber threats and risks at the human level and ensure the safety, inclusion, and continuation of women peacebuilders’ vital work. Political commitment matched with financial commitment from Member States, the UN, EU, other multilateral institutions, and stakeholders is necessary to make this happen.

Thank you