Statement to the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security
10 September 2019

It’s difficult to imagine another topic as ubiquitous as information and communications technologies, or ICTs. Their integration into nearly every facet of our lives makes their vulnerability—and relatedly, our vulnerability—to attack or misuse so great.

Which is why the Women’s International League for Peace and Freedom (WILPF) is pleased to see the establishment of a new entity within the UN system that will take up this subject, and one that will conduct its work in an open manner and a method inclusive of the entire UN membership and other stakeholders. This is not a subject that can be held hostage by a few powerful states or actors. It affects us all in ways more immediate than even some of the other security and weapons discussions that are had here in this room.

That said, we strongly regret the absence of several members of global civil society today, as a result of a broad denial for accreditation to any organisation or entity not possessing ECOSOC status. Such a broad and categorical denial of access is extremely rare in UN disarmament and arms control fora and sets a dangerous precedent.

WILPF wishes to set out the following five messages for member states participating in the OEWG:

1. WILPF is increasingly concerned by the militarisation of cyber space and supportive of solutions that move us closer to cyber peace. WILPF believes that the pursuit of cyber peace necessitates processes that will understand cyber space on its own terms and consider its specific characteristics, including its overwhelmingly civilian nature, by avoiding an approach that unnecessarily imports concepts from traditional disarmament and arms control. The slow creep of disarmament and national security-first language into this landscape demonstrates and simultaneously reinforces, the extent to which we are collectively allowing cyber space to become militarised. It implies a tacit acceptance of the weaponisation of technology, an approach that will exacerbate or create violence in a new medium where it does not necessarily otherwise occur.

2. In line with the above, WILPF encourages member states to identify solutions and approaches that reduce the motivation to pursue aggressive cyber capabilities, such as through positive obligations or confidence building, and
encourages efforts to break through the playing of politics on this issue. Inclusivity and transparency are imperative.

3. WILPF recommends that the humanitarian and human rights impact of cyber operations be a guiding principle and central to multilateral discussions of cyber peace and security rather than being treated as a secondary after-thought. It’s vital that the OEWG does not overlook the real-life repercussions that malicious intergovernmental operations can have on citizens. That said, better research and information gathering on the humanitarian impact of such operations should be encouraged. There is however, an ever-growing and highly credible evidence base illustrating the negative uses of digital technology in repressing human rights, notably the rights to freedom of expression, speech, assembly, and privacy. While the human rights part of the cyber agenda is rightly being pursued in other forums it cannot be separated entirely from discussions in the First Committee.

4. It is regrettable that the outcomes of earlier UN bodies on this subject are not being reflected in the actual conduct of states in cyber space and there is an increase in the number of offensive cyber operations occurring between states, including that which targets civilian infrastructure. Adherence to already agreed behavioural norms, including by some of the same states who advocated for their development, and more attention to attribution mechanisms, is necessary.

5. As an organisation that has long been at the forefront of feminist advocacy for disarmament, WILPF also wishes to highlight the gender aspects of this issue. At a societal and individual level, digital networks are being used to harm people on the basis of gender in new and disturbing ways. With the emergence of social media in particular, sexual and intimate partner violence have taken on new dimensions that include bullying, defamation, impersonation, surveillance, tracking, and harassment as well as non-consensual sharing of photos or messages. Online gender-based violence (GBV) is often directed at those who break from—or are perceived as breaking from—traditional gender norms in any range of ways. In some contexts, online GBV is exacerbated by the anonymity that an abuser can have on a social media platform; whereas in others it is bound up in other forms of intimate partner violence and used as a form of control.

The work of the OEWG will not be easy. It will need to reconcile parallel discussions occurring in the concurrent sixth Group of Governmental Experts as well as the evolution of normative and legal discussions in other, non-UN spaces. It will also need to find a way to break beyond the deadlock and antagonism of earlier UN discussions.
on cyber security as well as those that exist in reality between some of the same states that are most active in this area, either for their poor conduct or past efforts to develop rules, norms, and principles. Yet at the same time the opportunity is great and the urgency is real; we appeal to member states to seize this opportunity to prevent the growing militarisation of cyber space and orient instead towards cyber peace, based on human security.