Statement by Media Foundation for West Africa at the 2nd Substantive Session of the Open-Ended Working Group of the United Nations

The Media Foundation for West Africa (MFWA) is grateful for this opportunity. The Media Foundation for West Africa is an independent, regional Non-Governmental Organisation based in Accra, Ghana. It promotes and defends the right to freedom of expression of all persons, particularly the media and human rights defenders in West Africa.

Over the past two decades, democratic transitions have been on the rise in West Africa and with it a significant improvement in the respect for fundamental human rights. The internet has improved the lives of the people in West Africa. Not only have their freedom of expression, freedom of association, and freedom of assembly rights have been strengthened, but their economic rights (e-commerce), education (e-learning) etc. The internet has also given room to more participatory, accountable and transparent governance with the advent of e-governance platforms and systems.

Mr Chair, while concerns over terrorism, fundamentalism, cybercrime, hate speech, misinformation and disinformation are legitimate, they must not be used to violate human rights of individuals in the cyberspace. Neither should their online engagements lead to their offline harassments. There is a growing threat of journalists, human rights defenders and activists who report on terrorist activities and are critical of governments being tagged as “enemies of the state” and targeted as ‘cyberthreats’ themselves.

Actions such as arbitrary surveillance of journalists, media, human rights defenders and others, must be condemned. Mass surveillance used by states as a reaction to cyberthreats is not a human rights respecting response to threats. Threats in cyberspace should be seen from a rights-based approach and measures to counter these threats should focus on ensuring accountability for state behaviour in cyberspace, inline with international law.

In this regard, we appeal to the OEWG to call on states to cease using state law enforcement institutions such as police and judiciary, to cause the arbitrary arrests/detentions of journalists, citizens, and activists and levelling cybercrime charges against them. As the Freedom Online Coalition joint statement on the Human Rights Impact of cybersecurity laws, practices and policies recommends;
“States need to develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists. This includes building, where appropriate, supporting processes and frameworks for transparency, accountability, judicial or other forms of independent and effective oversight, and redress towards building trust.”

There is, therefore, the need to ensure that states refrain from wrongful use of cyber-related policies to silent critical voices. States should also recognize that international human rights law extends beyond the duties of states to include the responsibility of businesses to respect human rights and abide by their due diligence to ensure that their products and services are not used to violate human rights. In line with the UN Guiding Principles on Business and Human Rights, States should be willing to share information about human rights abuses by private actors and should hold private actors who enable or facilitate these acts to account.

As Norm E in the 2015 GGE report highlights,

“States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.”

Therefore, governments should ensure that violations against human rights online by both state and non-actors (such as the private sector) in the cyberspace are monitored, thoroughly investigated and addressed.

In line with this, capacity building measures should include state institutions that have the mandate to promote, and protect human rights are adequately resourced and strengthened to not only deal with cyberthreats but to also use their mandates to promote human rights when it comes to cyberthreats and cybersecurity issues more widely.

More measures are needed to create awareness on cyberthreats, and initiate capacity-building measures aimed at increasing digital literacy of citizens. Civil society organisations, particularly, should be seen as good partners in capacity-building and awareness raising interventions on cybersecurity.
Mr Chair, when it comes to stakeholder engagement in the development of cyber-related legislations and policies, we wish to reiterate the importance of ‘meaningful stakeholder engagement’, which requires timely information sharing, transparency, accountability and engagement of stakeholders throughout the development and implementation of processes.

Mr Chair, human-rights should be at the centre of cyber policy development and implementation and we urge greater transparency, accountability, and inclusivity in these discussions.

Thank you, Mr Chair.