



Global Digital Compact. Such measures to collaboration and cooperation.

The CyberPeace Institute welcomes the call for civil society organizations to contribute to the Global Digital Compact and respectfully provides the following recommendations:

1. **Multistakeholder governance: Build on existing frameworks, and build on existing** international frameworks, and to reinforce and reaffirm existing

commitments but should not duplicate existing work, mandates or norms.


Peace and security in cyberspace requires a collective effort and meaningful multistakeholder cooperation including from civil society organizations, industry actors, academia, and experts. Civil society actors already play a critical role in the provision of expertise and guidance in relation to the stability of cyberspace, the impact on human rights and people's security, and are integral to the functioning and integrity of many of the existing digital cooperation frameworks. Thus, a multistakeholder approach to developing, and implementing, the Global Digital Compact should be facilitated. Procedural modalities shape the substantive discussions and how States interact with stakeholders, and the participation of relevant actors, including the private sector, civil society and academia, should be incorporated in a formal, comprehensive, and systematic manner.

2 Apply human rights online: Ensure a human-centric approach and reinforce existing

The cyber threat landscape is rapidly evolving with a rise in the frequency, sophistication and intensity of cyberattacks in situations of armed conflict and peace with the risk of real harm to people, and severe humanitarian consequences.

Cyberattacks and cybercrime are exploiting the interconnectedness and digitalization of our societies and blur the boundaries between perceptions of peace and conflict. The security of cyberspace is essential for a stable global system, thus action must be taken to strengthen this security with approaches that enhance trust, the rights of people and societal resilience. The unique nature of cyberspace requires a collective responsibility from all sectors of society to ensure the respect of laws, rights and norms for the protection of people.

The creation and dissemination of hate speech, disinformation and misinformation undermines access to information, par n



awareness, digital literacy and skills, cyber-hygiene and online safety practices. The importance of a multistakeholder approach involving the public sector, international organizations, civil society, industry, and other actors should be underscored by the Global Digital Compact as essential to understanding, identifying scalable solutions and addressing the challenges.

The Global Digital Compact should encourage a multidisciplinary approach across sectors including the cybersecurity and development communities, to achieve "cyber resilience for development". Cybersecurity needs to be mainstreamed into the international development agenda as core enablers of digital, economic, and social development.