Contribution from the Global Forum on Cyber Expertise (GFCE)
April 2023

On behalf of the Board of the Global Forum on Cyber Expertise (GFCE) Foundation, we submit the following contribution to the Global Digital Compact. The GFCE appreciates that the consultative process on the Global Digital Compact is inclusive and transparent, ensuring that the consensus on shared principl   es for an open, free and secure digital future for all.

The GFCE is a neutral, apolitical platform for international cooperation and exchange on strengthening cyber capacity and expertise globally. Established in 2015, its multi-stakeholder network comprises of over 190 organizations including governments, civil society, academia, private sector, and international organizations. On this occasion, we respectfully provide input on digital connectivity for your consideration.

1. Connect all people to the internet, including all schools

development and human rights for all people. [?]
realization of the 2030 Agenda for Sustainable Development
digital connectivity comes with challenges and risks, a[?]
malicious actors. Therefore, the GFCE advocates for [?]

as crucial elements of digital connectivity, as they enable countries and communities to protect themselves from cyber threats and vulnerabilities, develop skills, and harness the opportunities of cyberspace.

Core Principles for Governments, International Organizations, Businesses Universities and Other Relevant Stakeholders

- Digital connectivity is a key enabler of sustainable development that should be available, affordable, accessible, and meaningful for all people.
- Ensuring universal access to the internet should be a priority for all nations, especially prioritizing marginalized communities (e.g. women and girls, remote and rural communities, ethnic minorities and indigenous people, persons with disabilities, older people).
- Bridging the digital divide requires collaboration between governments, the private sector, civil society, and other stakeholders.
- Cybersecurity and cyber capacity building are essential components of digital connectivity, as they ensure countries and communities can protect themselves from cyber threats and vulnerabilities, and fully leverage the benefits of cyberspace.
- Cyber capacity building should follow a multi-stakeholder, inclusive and human-centric approach that involves collaboration and coordination among governments, international

organizations, non-governmental organizations, civil society, private companies, the technical community and academia. [1]

Key Commitments, Pledges, Actions

-