Global Digital Compact: Submission from the CyberPeace Institute

The CyberPeace Institute, an independent and neutral non-governmental organization headquartered in Geneva, Switzerland, has a mission to reduce the harms from cyberattacks on people’s lives, provide assistance to vulnerable communities, and call for responsible cyber behavior and accountability. In a world where the use of digital technologies is increasingly becoming ubiquitous it is important that their use serves humanity and does not undermine it. This requires 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 mainstream a multistakeholder approach

The Global Digital Compact is an opportunity to bring together different policy areas and fields of international law within the United Nations system, to increase coherence 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.

© 2023 CyberPeace Institute. All rights reserved
2. **Apply human rights online: Ensure a human-centric approach and reinforce existing protections for human rights**

The maintenance of international peace and security needs to ensure the protection and enablement of individuals and communities to enjoy their fundamental rights and freedoms, including rights to economic and social advancement, in cyberspace. This will require the acknowledgment of a human-centric approach to security of and in the use of ICTs and to facilitate a more comprehensive understanding of the impact and harm of the malicious use of ICTs on people and society.

Human rights, protected by the international human rights framework, are applicable online and offline, yet digital technologies are being used to restrict freedoms and violate human rights, for example, through unlawful surveillance, disinformation, hate speech and online abuse, internet shutdowns, unlawful collection or misuse of data. The Global Digital Compact must reinforce the existing international human rights framework, and focus on implementation and advancing of human rights online, including freedom of expression, non-discrimination, freedom of assembly, privacy and to seek, receive and impart information. Relevant international human rights frameworks include the *Universal Declaration of Human Rights*, the *International Covenant on Political and Civil Rights* and the *International Covenant on Economic, Social and Cultural Rights* with their respective Protocols, the Conventions\(^1\) that layout in more detail these rights, and finally the *UN Guiding Principles on Business and Human Rights*.

It is important that international human rights law determines states’ and businesses’ responses to the use of digital technologies, for example, surveillance technology and the use of Artificial Intelligence. Increased transparency and accountability are very important, and States and businesses must take more action in this regard.

---

3. **Cybersecurity as collective security: A focus on the importance of cybersecurity for collective security, safety, and the respect of rights and freedoms**

\(^1\) International Convention on the Elimination of All Forms of Racial Discrimination (ICERD); Convention on the Elimination of All Forms of Discrimination against Women (CEDAW); Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment (CAT); Convention on the Rights of the Child (CRC); International Convention on the Protection of the Rights of all Migrant Workers & Members of their Families (ICRMW); Convention on the Rights of Persons with Disabilities (CRPD); International Convention for the Protection of All Persons from Enforced Disappearance (CED)

© 2023 CyberPeace Institute. All rights reserved
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, participation online, and can constitute incitement to hostility, discrimination, or violence, with devastating consequences for people and communities online and offline. The vulnerability of different individuals and groups differs according to their exposure to a given problem, the impact on them and their capacity to tackle it. Religious and ethnic minorities, and marginalized groups are often disproportionately impacted, with women and children facing compounding effects linked to specific vulnerabilities. Disinformation and misinformation can also increase the exposure of individuals or groups to other risks and vulnerabilities, for example, they may not seek life-saving support or assistance from organizations, such as IOs and NGOs, due to intentionally misleading information.

It is essential that the Global Digital Compact underscores the importance of upholding respect for human rights. Governments and the corporate sector need to respond to curtail hate speech, disinformation and misinformation, with approaches that focus on the implementation of human rights, promoting transparency and meaningful accountability accompanied by independent oversight. In this regard, the Global Digital Compact should play a role in ensuring a data and evidence-based approach, including gender disaggregated data, to understanding which interventions are impactful to curtail hate speech, disinformation, and misinformation, to share best practices, and to improve digital skills of users to identify and address harmful material. Multistakeholder partnerships will be vital for an effective and sustainable response to the spread of hate speech, disinformation and misinformation that respect human rights and a human centric understanding of safety and security. In addition, addressing gender based challenges will require transformative and inclusive solutions and approaches, including to ensure women’s participation.
4. Avoid Internet fragmentation: Preserve the universal character of the Internet

The fragmentation of the Internet creates boundaries in cyberspace. It undermines the Internet as a motor of economic and social development, increases the risks of an information vacuum and the spread of misinformation and disinformation, and poses risks for the respect of human rights and security. The Internet’s openness depends on trust and this trust is undermined when access to the Internet is blocked for political or other reasons including in times of war or other crises.

The open, multistakeholder model of governance of the Internet through a number of different organizations, companies and international fora is primordial in protecting a free, open Internet for all. The Internet’s strength is its distributed nature. All efforts must be made to preserve the universal character of the internet, and to prevent activity that damages the availability and/or integrity of the public core of the internet. In this regard, it is critical that the multistakeholder, decentralized approaches to the current model of the Internet are reinforced.

The Global Digital Compact should reaffirm the multistakeholder decentralized approach for the governance of the Internet, and preserve the principles of openness, availability, and integrity of the Internet.

5. Connect all People: Digital Inclusion, Connectivity, and Capacity Building

People need inclusive, meaningful and secure connectivity, knowledge and tools to ensure their ability to tap into the potential of digital technologies. These conditions are also critical to the achievement of the Sustainable Development Goals (SDGs). Digital connectivity is a key enabler of social and economic development and underpins the achievement of the SDGs, yet the digital divide persists. The Global Digital Compact should support efforts to foster inclusive connectivity and there is a critical need for international cooperation and to understand in each context the factors that contribute to the connectivity gap and digital divide.

Benefiting from digitalisation while strengthening societal and cyber resilience requires international collaboration, capacity building at all levels putting inclusion and people at the center, addressing the digital divide, and the sharing of best practices and investment.

The Global Digital Compact should encourage and facilitate the development of multistakeholder solutions and cooperation to tackle digital divides, promote digital
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.