Our submission to the UN Secretary General's High-level Panel on Digital Cooperation

GLOBAL PARTNERS DIGITAL

About Global Partners Digital

The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities. Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Our submission

GPD welcomes the UN Secretary General's High-level Panel on Digital Cooperation's Call for Contributions to inform its deliberations and development of actionable recommendations for its report. In this submission, we outline the values and principles we believe should underpin digital cooperation, and we draw on our experience engaging with stakeholders to offer analysis of the challenges, constraints and gaps faced by stakeholders in achieving digital cooperation, as well as recommendations on how these can be overcome. Finally, we focus on the illustrative action areas "digital trust and security" in section 3, where we describe the main challenges faced by stakeholders with regards to digital trust and security, refer to examples of successful cooperation in this area, and suggest the values and principles that should underpin cooperation in this area.

1 Values & Principles

Question 1(a): What are the key values that individuals, organizations, and countries should support, protect, foster, or prioritize when working together to address digital issues?

Global Partners Digital (GPD) believes that the most important values that individuals, organisations and countries should support, protect, foster and prioritise when working together to address digital issues are human rights. The internet and other digital technologies have the potential to enhance greatly the enjoyment and exercise of almost all human rights, from the rights to freedom of expression, association and assembly, to the rights to education and highest attainable standard of health. It is also well-recognised and accepted that "the same rights that people have offline must also be protected online".

However, these technologies can also be used in ways which restrict human rights or developed and regulated in ways which undermine their potential to fully deliver the benefits that they can offer. In recognition of this, ensuring that human rights are respected, protected and promoted is fundamental when it comes to all aspects of cooperation on digital issues from their design to their application to their governance, including by way of regulation.

In addition to human rights broadly as values, we also believe that there are further values, which we set out below, which are also important, although they can also be seen as supporting the broader values of human rights.

- **Equality and diversity:** The internet and other digital technologies should not introduce or exacerbate divides between people, offline or online, or exclude people based on any ground such as - but not limited to - race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, sexual orientation, gender identity, disability and health status. Cooperation on digital issues should seek to promote equality, in part through meeting needs of the full diversity of users and potential users, including cultural and linguistic diversity.

- **Openness:** The internet and other digital technologies should be designed, applied and governed, as far as possible, to support the ability of users to seek, receive and impart information and ideas of all kinds. Cooperation on digital issues should recognise this as one of the core purposes of such technologies. Further, where cooperation on digital issues relates to the development of the infrastructure of or standards relating to the internet and other digital technologies, such cooperation should be as open and inclusive as possible, to ensure that the needs and perspectives of users and potential users are considered.

- **Security and resilience:** Strong security and resilience of the infrastructure, networks systems and information which the internet and other digital technologies operate upon and use helps protect not only those physical and digital elements, but also their users, particularly their privacy. As such, their design, application, and governance, as well as cooperation on digital issues, should promote the security of users themselves.

Question 1(b): What principles should guide stakeholders as they cooperate with each other to address issues brought about by digital technology?

In order to help fully realise the values listed above, the following principles should guide the cooperation of stakeholders when addressing issues brought about by the internet and other digital technologies.

- **Openness and accessibility:** Cooperative processes should be open and accessible to all relevant stakeholders. This may take the form of active measures to enable participation (e.g. notice given well in advance and distributed via relevant channels), as well as efforts made to address obstacles that may prevent or discourage it.

- **Inclusiveness of stakeholders' views:** Cooperative processes should ensure that the different views and interests of the relevant stakeholders are heard and considered, and that deliberations are informed and evidence-based.

- **Consensus-driven:** Cooperative processes should require participants to act with common purpose, in a collaborative manner and, as far as is possible, take decisions by general agreement. Compromise also plays an important role.

- **Transparency and accountability:** Cooperative processes should include clearly defined and transparent procedures and mechanisms. These can include disclosure of stakeholder interests, systems of records management, clear and functioning lines of accountability internally between the leadership and group, as well as externally between stakeholders and their wider communities.

Question 1(c): How can these values and principles be better embedded into existing private and/or public activities in the digital space?

These values and principles can be embedded into private and public activities in the digital space through application of the international human rights framework and a multistakeholder framework.

International human rights framework

The international human rights framework is a body of law and standards which set out how values of human rights should be respected, protected and promoted. While legally binding only upon states, it is now recognised also to set out the responsibilities of businesses, and serves as an important framework for determining how the values of human rights can be respected in other activities and by other actors.

The international human rights framework recognises a wide range of human rights, primarily found in three documents known collectively as the International Bill of Rights. These are the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. The rights within these documents have been further elaborated upon in further issue- and group-specific treaties, including the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention on the Elimination of All Forms of Discrimination against Women, the Convention on the Rights of the Child, and the Convention on the Rights of Persons with Disabilities.

The importance and utility of the international human rights framework stem, in part, from the fact that this framework, and the treaties which underpin it, have been negotiated and agreed by states at the global level. When it comes to states, there are also a range of

monitoring and accountability mechanisms which are attached to them. Furthermore, the international human rights framework provides clarity and detail on the scope of individual human rights, sets out - where relevant - permissible limitations and restrictions - and details the steps and actions that must be taken in order for those rights to be fully respected and protected.

The international human rights framework comprises, in part, reports of UN special procedures, resolutions of the UN Human Rights Council, and General Comments of the UN Treaty Bodies, which help interpret the treaties which underpin the international human rights framework, including in the digital age (please see Annex on p. 9).

For states, ensuring that any legislation or policies, as well as other state actions, relating to the internet and other digital technologies is consistent with international human rights law and standards is critical to ensuring that human rights are respected and protected. Such an approach also supports cooperation on digital issues, by ensuring a consistent approach across jurisdictions.

As noted above, although the international human rights framework is only legally binding upon states, this does not limit its relevance to other actors. It is recognised that due to the important role that the private sector plays when it comes to human rights, businesses have a responsibility to ensure that they do not adversely impact human rights and should seek to avoid such adverse impacts. More guidance on how this can be done is outlined in our response to question 2(a).

The clarity and detail that the international human rights framework provides on how human rights should be respected and promoted also means it can be beneficial to other actors - such as international organisations and multistakeholder partnerships - who engage on issues relating to the internet and other digital technologies, despite not having legal obligations or responsibilities under the framework.

Multistakeholder framework

The principles set out in our response to question 1(b) draw from commitments to a multistakeholder approach which has been acknowledged to be a cornerstone of internet governance processes in a range of high-level documents including the Tunis Agenda and the high-level review of the WSIS.

Although it has no single definition, the multistakeholder approach refers to a distributed policymaking model based on the cooperation of key actors and stakeholders. The flexibility and openness of multistakeholder principles are particularly relevant to cooperation on digital issues due to the global nature of the internet which implicates a wide range of actors, across jurisdictions. Although not as defined in the same way as the international human rights framework, and lacking comparable institutions and mechanisms, the principles are an important complementary reference to it.

GPD has developed a framework (4) which distils the different characteristics which define a multistakeholder process. Some examples of how the GPD multistakeholder framework has been successfully applied are referred to in response to question 3(b).

2 Methods & Mechanisms

Question 2(a): How do the stakeholders you are familiar with address their social, economic, and legal issues related to digital technologies? How effective or successful are these mechanisms for digital cooperation? What are their gaps, weaknesses, or constraints? How can these be addressed?

Private sector

Private sector actors address social, economic, and legal issues related to digital technologies in a range of ways:

- Undertaking risk assessments and impact assessments when designing or refining their products, services and applications;
- The development of company policies and processes;
- The ways in which they seek to conform to the legal and regulatory environments in which they operate;
- Cooperative mechanisms and initiatives with other actors and stakeholders, both private and public, such as the Global Network Initiative and Tech Against Terrorism.

There are a number of gaps, weaknesses and constraints when it comes to private sector actors addressing social, economic, and legal issues related to digital technologies, including:

- A lack of understanding, particularly among small and medium enterprises, of international human rights law and standards, and the responsibilities of private enterprises under the United Nations Guiding Principles on Business and Human Rights;
- When seeking to ensure compliance with the legal and regulatory environments in which they operate, ambiguity or - sometimes - the lack of legal and regulatory frameworks which apply within the particular jurisdiction;
- In addition to the above, for private sector actors operating across multiple jurisdictions, the existence of conflicting legislation and regulation;
- The existence, in many jurisdictions, of applicable legislation and regulation which is inconsistent with international human rights law and standards, risking complicity by private sector actors;
- A lack of transparency of companies' actions - including internal policies and processes; the development and use of algorithms; the collection, use and sharing of users' data - making it challenging for other actors to engage with private sector actors.

These gaps, weaknesses and constraints can be addressed, inter alia, by:

- Better understanding and implementation of the United Nations Guiding Principles on Business and Human Rights by private sector actors, including through the development of human rights impact assessments;
- Reviewing good practices from other private sector actors that have already been developed;
- Identifying potential adverse impacts related to a private sector actor's activities or business relationships through human rights impact assessments and other forms of due diligence;
- Better engagement with other relevant stakeholders, particularly civil society organisations, potential victims and at-risk groups;
- Developing meaningful grievance and remedial mechanisms for when adverse human rights impacts occur;

- Publishing regular and meaningful information and data in relation to their actions which have an impact upon human rights, such as when personal data is shared with third parties, when content on a platform is removed or restricted, when access to particular services are blocked or restricted;

Governments also have a key role to play through the development and implementation of National Action Plans on Business and Human Rights, which specifically recognise the particular issues relating to the internet and other digital technologies, as well as appropriate legislative and regulatory frameworks which ensure that human rights are protected in the private sector.

Governments

Governments also address social, economic, and legal issues related to digital technologies in a range of ways:

- The development, implementation and revision of national-level legislative, policy and regulatory frameworks;
- Binding and non-binding agreements with other states to address issues related to digital issues, including bilateral treaties (such as mutual legal assistance treaties), multilateral treaties (such as the Budapest Convention on Cybercrime) and international alliances (such as the Freedom Online Coalition);
- Engaging, including through agreements, with private sector actors.

There are a number of gaps, weaknesses and constraints when it comes to governments addressing social, economic, and legal issues related to digital technologies, including:

- A lack of open, inclusive and transparent processes in the development and implementation of relevant national strategies, for example national cybersecurity strategies;
- A lack of harmonisation of regulatory frameworks with international best practice;
- Instances of inappropriate 'copying' and 'pasting' legislation from one jurisdiction to another, which can lead to gaps in safeguards for human rights where the second jurisdiction doesn't have the same safeguards as the first;

These gaps, weaknesses and constraints can be addressed, inter alia, by:

- Instituting open, inclusive and transparent processes (see Global Partners Digital, Multistakeholder Approaches to National Cybersecurity Strategy Development);
- Ratifying and implementing best practice global and regional in order to harmonise regulatory frameworks;
- Ensuring adequate safeguards for the protection and promotion of human rights in legislation;

Question 2(b): Who are the forgotten stakeholders in these mechanisms? How can we strengthen the voices of women, the youth, small enterprises, small island states and others who are often missing?

We understand the term 'underrepresented groups' and 'forgotten groups' as referring to groups which are not sufficiently represented in discussions relating to digital technologies, often due to existing constraints and challenges which pre-date the digital age. These include older persons, those on low incomes, women, young people and disabled people. The extent of disparity or exclusion of these groups will however vary or depend on context, including national or cultural context.

This underrepresentation stems from a number of factors and cannot be effectively addressed through one measure alone. Complicated issues relating to power dynamics, and structural inequalities and barriers can hinder equal access and participation of certain groups in discussions - even when these discussions directly relate and impact the groups in question.

There are, however, some overarching considerations which should be borne in mind when efforts are made to strengthen the voices of underrepresented groups. Any efforts should promote transparency and accountability of decision-making processes and mechanisms so that underrepresented stakeholders have the necessary information to be involved. Providing information alone will not, however, be sufficient. When it comes to participation, cultural, social, economic and barriers are linked. Therefore, there must be sensitivity to the multiple barriers that can inhibit participation. For example, in some parts of the world, women may be inhibited because of social and cultural norms which remove or limit their ability to participate in spaces that are not related to the family or community. Simply inviting women to participate, for example, will not address these issues. Any responses to overcoming these should be evidence-based, in particular evidence informed through participatory research methods that involve the communities in question. They should also consider the broader legal and regulatory framework which shape opportunities for participation in decision-making processes. For example, in some parts of the world, civil society are barred from participating meaningfully through legal restrictions on receiving foreign funding, or restrictions on the types of activities they can undertake.

We would specifically recommend to the High Level Panel on Digital Cooperation that they review existing research into the closing of civic space worldwide which detail the challenge and offer recommendations. This research includes that undertaken by the International Consortium on Closing Civic Space (1), Open Global Rights (2), and the Civicus State of Civil Society Reports (3) (see links in Annex).

Finally, responses and efforts to meaningfully increase inclusivity and the voices of forgotten groups should be developed with sustainability in mind: one-off capacity building programmes, or one-off funding opportunities to participate in meetings or processes will not strengthen voices. Instead, outreach to under-represented groups and commitment to their inclusion and participation should consider how their capacity can be built and how they can be included in processes in the medium- and long-term through multi-pronged approaches.

Question 2(c): What new or innovative mechanisms might be devised for multi-stakeholder cooperation in the digital space?

See our response to question 3(c).

3 Illustrative Action Areas

Question 3(a): What are the challenges faced by stakeholders (e.g. individuals, Governments, the private sector, civil society, international organizations, the technical and academic communities) in these areas?

While there is a wide range of challenges that different stakeholders face when addressing or cooperating on digital issues, we wish to highlight one in particular, namely the narrative that frames many debates and policymaking processes when it comes to digital trust and security. In our experiences, the narrative that frames such debates and processes is heavily securitised, by which we mean that 'privacy' and 'security' are seen as two values which must be traded off against one another. Under such a framing, any efforts to increase security invariably necessitate a reduction in individual privacy. We have seen such a framing used by governments across the world. Approaching issues of digital trust and security in such a way

poses risk to individual security and the protection of human rights, and makes it more difficult for stakeholders who advocate for strong protection of human rights to engage in such debates and processes.

There are two specific policy areas where such framing has been prominent: encryption and state-sponsored hacking.

Encryption is one of the most important enablers of digital trust and security. We consider cybersecurity to mean the protection of information and its underlying infrastructure so as to enhance the security of persons both online and offline. Strong encryption ensures that the elements of cybersecurity are preserved, protecting both personal security and human rights. Strong encryption ensures that information is not modified by unauthorised means since it protects the integrity of information whether in transit or at rest. Strong encryption also ensures that information remains confidential by protecting it from authorised access. Finally, by protecting the integrity of information, strong encryption also indirectly protects the availability of information, by ensuring that information and systems are not tampered in a way that makes the information unavailable.

However, there have been, and continue to be, attempts by a number of governments to undermine the availability of strong encryption to individual users, including through legislative and regulatory measures. These includes attempts to compel companies to build 'backdoors' into their software, requirements sometimes also referred to as 'exceptional access'. These attempts have been made using arguments that any reduction in privacy is justified by the enhanced protection of national security and public safety, and with little recognition of the risks to security, including personal security, from such measures.

There has also been an increased use of hacking by a range of state actors in the absence of a clear legal framework or adequate safeguards. These measures have purportedly been adopted in response to the phenomenon of 'going dark', which is the term used to describe the scenario where information becomes unavailable because it has been encrypted. Yet, hacking is a highly intrusive technique that is very difficult to use in a narrow, targeted way, and it relies on certain practices like the hoarding of information relating to software vulnerabilities. Again, the adverse impacts upon individuals' privacy are justified on the basis that national security overall is enhanced. However, practices like these weaken everyone's security because they lead to a risk of software vulnerabilities being leaked to the public, and being exploited by malicious actors before they can be fixed.

Challenges related to the access of data for legitimate purposes, should be addressed in a way that fully complies with international human rights law and standards. Efforts that should be made include greater use of vulnerability disclosure processes, and greater efforts to protect cybersecurity in a way which emphasise the protection of the security of persons both online and offline.

Question 3(b): What are successful examples of cooperation among stakeholders in these areas? Where is further cooperation needed?

Successful examples of multistakeholderism to promote cooperation in these areas include:

- The Global Commission on the Stability of Cyberspace (GCSC)
- The Global Forum on Cyber Expertise (GFCE)
- The GPD Framework for Multistakeholder Cyber Policy Development (https://www.gp-digital.org/publication/multistakeholder-framework/)
- The Internet Governance Forum's Best Practice Forum on cybersecurity
- Freedom Online Coalition Working Group on an "Internet free and secure" which developed through a multistakeholder process a series of recommendations for states on cybersecurity and human rights: (https://freeandsecure.online/)

Question 3(c): What form might cooperation among stakeholders in these areas take? What values and principles should underpin it?

In terms of the values and principles that should underpin cooperation, please see our response to question 1(c).

With regards to specific mechanisms that can promote cooperation in the area of digital trust and security at the global level, both the GFCE and the GSCS provide examples of how multistakeholder cooperation can support the development of innovative solutions to commonly agreed challenges.

These values and principles should also be applied to multilateral mechanisms. For example, the establishment of mechanisms within multilateral spaces like the United Nations (UN) can also draw on these examples. The establishment of a UN Group of Governmental Experts and an Open Working Group on "Advancing Responsible State Behaviour in Cyberspace" in November 2018 provides an opportunity. For example, a multistakeholder advisory board, housed within an existing UN-affiliated research institution, with clear terms of reference, could be established to feed into these processes.

In order to promote digital cooperation as well, governments should adopt national cybersecurity security strategies which clearly outline their plans for international cooperation on cybersecurity issues. In order to support the adoption of user-centric cybersecurity standards, all stakeholders should support the adoption of privacy by design principles for the processing of all types of personal information. These principles should be incorporated and implemented by states through comprehensive data protection legislation. Widespread adoption of strong and comprehensive data protection legislation can also promote digital cooperation by harmonising legal frameworks.

4 Any other ideas you would like to share with the Panel?

N/A

5 Please provide your numbered references or links to additional reports/documents here.

1. The International Consortium on Closing Civic Space: https://www.csis.org/programs/international-consortium-closing-civic-space-icon
2. Open Global Rights: https://www.openglobalrights.org/closing-space-for-civil-society/
3. Civicus State of Civil Society Reports: https://www.civicus.org/index.php/state-of-civil-society-report-2018
4. Global Partners Digital, Multistakeholder Approaches to National Cybersecurity Strategy Development: https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/

Annex:

UN Human Rights Committee General Comments

- Human Rights Committee, General Comment No. 16: Article 17 (Right to privacy) (1988)
- Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression (2011)

UN Human Rights Council Resolutions

- Human Rights Council Resolutions on the promotion, protection and enjoyment of human rights on the Internet (20/8, 26/13, 32/13 and 38/7)
- Human Rights Council Resolution on the right to privacy in the digital age (28/16 and 34/7)
- Human Rights Council Resolution on accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts (38/5)

UN Special Procedures

- Report of the Special Rapporteur to the Human Rights Council on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (2015)
- Report of the Special Rapporteur to the Human Rights Council on Freedom of expression, states and the private sector in the digital age (2016)
- Report of the Special Rapporteur to the Human Rights Council on online content regulation (2018)

Other Reports

- Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age (2014)
- Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age (2018)