

Global Digital Compact Asia Regional Consultation

New Delhi
March 21-22, 2023



United Nations
Office of the Secretary-General's
Envoy on Technology



**Ministry of
External Affairs**
Government of India



Federal Foreign Office

**Global
Digital
Compact**



Content

Introduction.....	0
Executive Summary: Main Findings and Outcomes	1
1. Welcoming Remarks. High-level intervention	6
1.1 Amandeep Singh Gill, United Nations Secretary-General’s Envoy on Technology	6
1.2 Abhishek Singh, CEO, National e-Governance Division, Ministry of Electronics and Information Technology India.....	6
1.3 Dr. Philipp Ackermann, German Ambassador to India	7
1.4 Muanpui Saiawi, Joint Secretary, Cyber Diplomacy, Ministry of External Affairs India	7
1.5 Dr. Regine Grienberger, Cyber Ambassador, Federal Foreign Office Germany.....	8
1.6 Ambassador Anna-Karin Eneström, Permanent Representative of Sweden to the UN	8
2. Workshop, Session, and Report Methodology.....	10
3. Work Session (a): Role of Digital Public Goods (DPG) including Digital Public Infrastructure (DPI) in the GDC to achieve the 2030 Agenda.....	12
3.1 How can emerging technologies and digital applications be used to address contemporary challenges?	12
3.2 How can the GDC facilitate sharing of Digital Public Infrastructure and/or Digital Public Goods among Member States?	13
3.3 How can DPIs promote innovation by the private sector including MSMEs and what constitutes the basic building blocks of DPIs?	15
3.4 What level of contribution is expected from stakeholders to build sustainable economic development models using digital technologies?	16
3.5 How can the global development community channel dedicated funding for the development of a DPI ecosystem?.....	17
3.6 How can DPIs and digital technologies be used for the development of low- and middle-income countries?	18
4. Work Session (b): Inclusive, open, accessible, safe, and affordable digital technologies and infrastructure and their co-governance	19
4.1 What is the role of stakeholders in ensuring inclusive, open, accessible, safe, and affordable digital technologies?.....	19
4.2 Which short-term measures are necessary and how can the GDC address this?.....	21
4.3 How can emerging technologies and digital applications be used to address contemporary challenges?	22
5. Work Session (c): Co-Governance model for developing Global Digital Cooperation with trust, security, and resilience	24
5.1 What kind of cooperation and collaboration is suitable for ensuring trust, security, stability, and resilience in digital technologies?	24
5.2 How can the GDC contribute to developing global digital cooperation?	24

5.3	What kind of cooperation and collaboration is suitable for ensuring trust, security, stability, and resilience in digital technologies?	25
6.	Work Session (d): Inclusion and Gender Equality in global digital transformation	27
6.1	How can we ensure inclusive participation?	27
6.2	How can bridge the digital gender divide?.....	28
6.3	How can risks and challenges such as gender-based online violence be addressed?	29
6.4	How can we increase/ensure digital literacy, awareness, and skills?.....	30
7.	Work Session (e): Impact of artificial intelligence, machine learning, and emerging technologies on online/offline privacy and protection.....	32
7.1	What are the risks associated with AI, ML, and other disruptive technologies to online/offline privacy?	32
7.2	How can AI and ML be used to identify and fight against misinformation and disinformation which may be generated by AI and ML?	33
7.3	How can emerging technologies be used to protect against online crimes?.....	34
7.4	What is the role of the GDC in ensuring safeguards?.....	34
7.5	How can the GDC guide the development of a regulatory environment to build future ‘privacy by design’ technologies?	36
8.	Work Session (f): Bridging the capacity gap for developing countries in the emerging technologies domain.....	37
8.1	How can collaboration and sharing of technology and resources with developed countries look like?	37
8.2	How should governments contribute to capacity building through funding, policies and infrastructure development?	37
8.3	How can local innovation and entrepreneurship be incentivized?.....	38
8.4	Which partnerships are required with the private sector and research organizations?	38
8.5	Which mechanisms are necessary to access international knowledge-sharing and collaboration?	39
8.6	What is the role of academia and industry to address the capacity gap?	39
8.7	How can capacity-building be implemented to strengthen developing countries' position on emerging technologies?	40
8.8	How can the GDC recommend sustained capacity development measures that are attainable	40
9.	Work Session (g): Security by Design: Technologies that can be scalable and affordable	41
9.1	What are the risks associated with open and accessible technology?	41
9.2	What are the present concerns on cyber security and the safety of digital technologies?	41
9.3	How can the GDC recommend ‘basic security and safety’ measures that could be incorporated into designing technologies?.....	42
10.	Work Session (h): Capacity Building for developing countries in cyber security	44
10.1	What are the mechanisms to strengthen human resources in cyber security at scale and affordable cost?	44
10.2	How can universal implementation of cyber security among all countries be achieved?	44

11.	Closing Remarks	46
11.1	Muanpui Saiawi, Joint Secretary, Cyber Diplomacy, Ministry of External Affairs India	46
11.2	Ambassador Anna Karin Eneström, Permanent Representative of Sweden to the UN	46
11.3	Regine Grienberger, Cyber Ambassador, Federal Foreign Office Germany	46
12.	Conclusion and perspectives towards the future	47
Annex.	48

Introduction

The Global Digital Compact (GDC) - Asia Consultations took place on March 21st and 22nd, 2023 in New Delhi, India. Similar consultations have taken place earlier for Africa (in Kenya, December 2022) and The Americas (in Mexico, February 2023). These consultations will lead to the Ministerial Meeting on the Summit of the Future (September 2023) and Summit of the Future - Global Digital Compact (September 2024). Participants for GDC Asia Consultations included stakeholders from government, civil society, private sector, academia, and international organizations, and had the following objectives:

- Contribute to the exchange of ideas about the potential as well as the challenges in the future use of digital technologies.
- Develop actionable inputs regarding digital inclusion to be included in the framework of the Global Digital Compact.
- Create a shared vision of the challenges and priorities of Asia regarding digital transformation.

Executive Summary: Main Findings and Outcomes

The two-day-workshop was preceded by a preparation call for participants on March 17th, 2023, clarifying its context, its objectives and its agenda as well as the participants' expectations and questions. The workshop itself took place with approximately 50 participants from governmental institutions, the private sector, non-governmental organizations as well as academia and research. At the core of the workshop were eight thematic sessions (sessions a - h), during which participants discussed and wrote down their input based on guiding questions. The main results of these exchanges are summarized in the following segments.

Work Session (a): Role of Digital Public Goods (DPGs) and Digital Public Infrastructures (DPIs) in the GDC to achieve the 2030 SDG Agenda:

- **Emerging tech/digital applications for contemporary challenges:**

Emerging tech and digital applications already help - and can help more - in many ways, such as access to healthcare and finance for the underserved, vaccine delivery with drones, blockchain for credit score calculation, AI for agricultural product management, energy optimization, and carbon tracking (sustainability).

Emerging technologies are customized for special needs, but such ad-hoc applications have limitations. Thus, foundational challenges of infrastructure, literacy, and affordability must be addressed for a bottom-up approach. Further, silos amongst and within governments must be addressed to have interoperable data and data standards. Fully representative data must be used as a shared resource (data commons) for contemporary challenges. GDC can play an enabling role in providing the digital common infrastructure such as data, data policy frameworks, and data exchange platforms.

- **Role of GDC in sharing of DPIs and DPGs among member states:**

GDC could facilitate and/or provide knowledge management services, capacity building, a network of expertise, and funding. Further, local needs must be understood – local capacity could be built with the participation of universities and civil society.

GDC could also promote and set standards for open, inclusive, and safe DPIs. The interoperability and scalability of DPIs must ensure 'privacy by design' and avoid vendor lock-ins. GDC could develop principles for the governance of DPIs towards fairness, and equity and disallowing new kinds of rent-seeking. It can also support the replication of DPI/DPGs between countries.

- **DPIs' promotion of innovation by the private sector:**

New products can be set up with a fraction of the costs (automation saves cost). Education for the youth is critical for the best usage of technology for innovation. Creating a good business model could encourage the private sector to participate in the DPI ecosystem. Having DPIs as a digital backbone will facilitate increased private sector contribution for innovation.

- **Level of contribution expected from stakeholders:**

The design of DGP/DPI should be rights-based, transparent by design, localizable, open to assessment by independent actors.

- **Funding for the development of a DPI ecosystem:**

DPI solutions must ideally have self-sustainable business solutions (with good revenue models and lessons from traditional project finance mechanisms) to avoid continuous reliance on grants/public funding. Funding must be democratic when provided – quadratic funding may be explored.

Dedicated funding and regional coordination facilities must be created. Funding must be consultative with the public, especially the most structurally vulnerable groups. The usage of public funding must be transparent, accountable, and open to critique and oversight.

- **DPIs/digital technologies for the development of low-and-middle-income (LMI) countries:** DPIs can enable scalability and capacity-building requirements of LMI governments, co-operatives, and civil society organizations, and last-mile service delivery. However, DPIs must understand local needs and values including that of structurally silenced groups – women, oppressed classes, disabled. Digital solutions for LMICs may need global cooperation and thus cannot be restricted to LMIC contexts.

Work Session (b): Ensuring inclusive, open, accessible, safe, and affordable digital technologies and infrastructure

- **Role of stakeholders:** Government must provide a level playing field to private actors, address areas of market failure, improve competition of each part of the digital connectivity value chain (avoiding monopoly), streamline access to the right of way and public sector connectivity infrastructure, track and punish exploitation enabled by tech (child abuse, etc.). However, the government's role may need to be reimagined due to its paternalizing factors. The private sector must view community networks as partners for creating new markets (instead of competition/threat) and invest in local content and platforms. Stakeholders must focus on human-centricity and inclusivity – especially the youth.
- **Necessary short-term measures with the role of GDC:** For existing DPIs, countries must implement/strengthen governance mechanisms where missing and/or deficient. For upcoming DPIs, establish governance mechanisms, advisory and safety panels before systems go live. Trade-offs need to be managed – safety v/s affordability; accessibility v/s safety. GDC may provide engaging and educative frameworks or modules for awareness and additionally provide consultations on changing and emerging technology.
- **Capacity constraints and solutions:** Education for technologists (engineers, designers) is not holistic – education with a broader worldview will enhance inclusivity. Low literacy affects accessibility – the design could be on speech or visual images. Presently, technology and internet applications are impliedly market-profit-centric – affordability needs to increase. There is a lack of programming knowledge on developing for people with disabilities that should be addressed.

Work Session c): Co-governance model for developing Global Digital Cooperation:

- **Suitable models:** Existing mechanisms within ITU/ICANN/G20/WEF could be strengthened with structural support by GDC to regional areas. The mechanism must be flexible but not changeable – a third-party body may oversee the system. Individual governments' feedback is necessary. Public authorities must not be upended from their legitimate governance role – Big Tech is getting too much of a governance role while it needs governance itself. Beneficiaries should also be able to vote on the technology and its features thereby increasing participation in the governance for developing digital cooperation.
- **Role of GDC:**

Define standards on what is a safe, accessible, trustworthy internet for stakeholders; and develop a framework and procedures for cross-border data flow for legitimate needs.

- **Elements needing common regulation/standards:**
Climate action; creating global talent pool; cross border labor mobility; e-commerce; cross border data flow; technical standards on accessibility and language.

Work Session (d): Inclusion and gender equality in global digital transformation

- **Ensuring inclusive participation:**
Understand gender beyond the traditional binary and ensure participation of most marginalized and intersectional vulnerable groups in consultative and decision-making processes. Potential barriers to participation must be addressed – limited access to tech, limited digital literacy, and barriers of language, behavior, culture, and social barriers. Address digital literacy by focusing on school curriculum including sexual and reproductive health rights as well as ensuring affordable digital devices and involve the private sector for awareness creation and upskilling.
- **Bridging the digital gender divide and addressing gender-based online violence:**
Adopt an intersectional gender approach to access and application of human rights online with special attention to online gender-based violence and gendered disinformation. Human-centric cybersecurity approaches could address online violence. AI models can be used to moderate online public forums and targeted programs to include women and girls in the development of emerging technologies. More specifically, AI models can reduce biases and stereotyping.

Work Session (e): Impact of AI/ML and emerging technologies on online/offline privacy and protection

- **Risks:**
Biases in AI/ML systems risk marginalization of certain sections - inherent human biases enter AI/ML systems and data sets are not crafted to address bias. Bias is related to exclusion and distributional issues – who gains or not (beneficiaries of tech-based welfare), who owns and controls, who just consumes. Privacy, limited access, copyright, and algorithmic black box are other risks. The existing gap in access to AI/ML by developing countries poses a risk, as well.
- **Usage of emerging tech:**
Cross usage of tech in designing risk management. For example, while AI is known for exclusion risks, blockchain can embed trust, transparency, and accountability. Online content's pattern analysis by AI fights mis-/disinformation.
- **Role of GDC in ensuring safeguards:**
GDC could gather best practices of AI use, harm, and benefits and harmonize existing and emerging regulations, standards, and guidelines.

Work Session (f): Building the capacity gap for developing countries in emerging technologies

- **Funding, policies, and infrastructure development:**
The focus must be on R&D and creating an ecosystem between industry, academia, and government. Publicly funded research must be made open source and must be made available

through global research networks. Academia must incentivize policy-relevant output, teach interdisciplinary courses (law and tech), utilize its reach to the youth, and support the marginalized. Global scholarships will incentivize researchers in underdeveloped/developing countries.

- **Incentivize local innovation and entrepreneurship:**

Streamline registration of startups, give tax incentives, share data pools for access, and provide opportunities in local projects. However, a culture of innovation must be embedded in education for long-term incentivization.

Work Session (g): Security by design: scalable and affordable technologies:

- Open and accessible technologies must be broadly defined but should not take away the agency from private parties for innovation and capability building. Further, open technologies need to be sustained with continuous contributions from those who have the capacity to adopt them locally.
- The present concerns of cybersecurity on digital technologies are for example: security and safety standards, fraud, fake news, cyberbullying, identity theft, and a lack of regulatory governance on cross-border tech companies.
- GDC can contribute to basic security and safety by furthering collaboration between sectors and developing high-level guidelines and principles with respect to human rights.

Work Session (h): Capacity building for developing countries in cyber security:

- Increase awareness by imparting digital literacy skills and developing training courses by expert volunteers. Further, the needs of all stakeholders must be understood – government, technical professionals, and general consumers. Simultaneously, jobs in governments and companies may be created to stimulate relevant demand. Universal implementation of cybersecurity could need enforceable treaties and conventions.
- Agreements, standards or treaties on cross-border cyber attacks and security can significantly contribute to the universal implementation of cybersecurity.

Day 1, March 21 2023

Global Digital Compact Consultations



1. Welcoming Remarks. High-level intervention

1.1 Amandeep Singh Gill, United Nations Secretary-General's Envoy on Technology

The UN Secretary-General's Envoy on Technology, Amandeep Singh Gill emphasizes the importance for the Global Digital Compact collaboration across different stakeholders, including governments, civil society, the private sector, academia, and the tech community, to imagine a digital future together. Mr. Gill highlights that the process is currently focused on listening and gathering inputs through the three regional consultations – Africa, America, and Asia – that are held in cooperation with the governments of Kenya, Mexico, and India. The Secretary-General will present a policy brief to the Member States and other stakeholders by the end of April, which will be reflected in an issue paper presented to ministers in September.

Mr. Gill emphasizes that the Global Digital Compact is one of several crucial outcomes that will be adopted at the Summit of the Future in 2024, which follows the SDGs summit, addressing the digital divide in all its aspects to accelerate progress on sustainable development.

He also highlights the importance of a shared vision to guide our actions, which can align the actions of different stakeholders across borders, but also across domains. The Tech Envoy stresses the significance of the regional consultations and inputs that reflect the particular regional context and the importance of said shared vision, if we are to accelerate progress on sustainable development and address the digital, connectivity and content divide as well as improve access to infrastructure and the security of our data. Addressing the participants, Mr. Gill points out the importance of the diverse group of participants that are present and their input to the discussions.

1.2 Abhishek Singh, CEO, National e-Governance Division, Ministry of Electronics and Information Technology India

Mr. Abhishek Singh discusses India's digital strategy, which has focused on leveraging technology to empower people and enable access to services focusing on how the use of digital technology has been critical in ensuring that people have access to safe services, even during the COVID-19 pandemic. India's digital strategy has focused on creating digital public goods and infrastructure. Further, the digital identity project, digital payments, and e-learning platforms are some of the initiatives also undertaken in the country. He reiterates that digital technologies have enabled access to services, inclusion, and empowerment of people at the grassroots levels in India.

Mr. Singh also emphasizes the importance of learning from other countries and collaborating to create digital public goods and infrastructure that work across borders. He mentions the creation of a common portal called "IndiaStack at Global" to showcase digital products and codes that are open-source and notes that India's digital efforts have been led not just by the government but also by the private and non-profit sector as well as entrepreneurs.

The CEO also highlighted that finding technical solutions - especially Digital Public Goods - is a journey of partnership and of working together and he hopes that the work will be continued in the same spirit driven by the United Nations and other global bodies and ensure that India becomes part of the consortium which helps in the adaptation on the digital public goods.

1.3 Dr. Philipp Ackermann, German Ambassador to India

Dr. Philipp Ackermann, German Ambassador to India, expresses gratitude to the Indian Ministry of External Affairs and the Joint Secretariat for their partnership in the Asia Consultations on the Global Digital Compact and highlights the commitment of the Indian and German governments to contribute to the GDC process with the aim of leveraging the full potential of digitization for achieving the 2030 agenda. He emphasizes that the Indian government shows leadership in the region by transferring shared principles of democracy and the rule of law into the digital world. Dr. Ackermann reiterates that the aims of the GDC are, to bring stakeholders together and to establish shared principles for an open, free, inclusive, and secure digital future, based on the principles of inclusiveness and transparency.

He acknowledges the challenge of regulating the internet and the importance of developing guidelines to prevent harmful misuse of technology. He then points out the harm that can be caused by misinformation and cyber attacks and therefore the significance to develop a set of guidelines that prevents harmful misuse of technology.

Dr. Ackermann proceeds to address the participants in the room, stating the importance that so many highly qualified experts from different stakeholders and various fields of expertise discuss in the coming days and a half about these very important matters. The Ambassador hopes that the participants will provide significant recommendations on multiple topics of the future GDC and emphasizes the importance of discussing these matters in person to have significant recommendations from the Asia Consultation for the Global Digital Compact.

1.4 Muanpuii Saiawi, Joint Secretary, Cyber Diplomacy, Ministry of External Affairs India

The Joint Secretary, Cyber Diplomacy, Ministry of External Affairs India, Ms. Muanpuii Saiawi welcomes the delegates to the Asian regional consultations to contribute to the United Nations Global Digital Compact, which is a framework for stakeholders to come together and work towards a more inclusive, equitable, responsible, and sustainable digital future. Ms. Saiawi notes that we are living in an age that is driven by technology, and the use of digital technologies in our daily lives has increased exponentially since the onset of the COVID-19 pandemic. She points out that the increased use of digital technologies has also created new forms of inequality, exacerbated existing ones, and raised important questions about privacy, security, and the protection of human rights.

She highlights that the GDC aims to ensure that digital technologies are used in responsible ways that promote economic, social, and cultural development, and aligns with the UN Sustainable Development Goals. The Joint Secretary focuses on key areas of action which include ensuring universal access to digital technologies, protecting personal data and privacy, promoting digital inclusion and literacy, and fostering innovation and entrepreneurship.

She points out that the agenda for the New Delhi consultations will focus on how the GDC and SDG 2030 can be set and implemented to the fullest potential and will address challenges such as the digital divide and ensure that the benefits are shared by all. Further, she hopes that the gathering will serve as a catalyst for further action toward a more sustainable and equitable digital future.

1.5 Dr. Regine Grienberger, Cyber Ambassador, Federal Foreign Office Germany

The German Cyber Ambassador, Dr. Regine Grienberger, is participating in the third round of consultations with Amandeep Singh Gill to prepare the ground for the Global Digital Compact. The ambassador believes that the Global Digital Compact helps in reaching the Sustainable Development Goals, especially digitization will be one of the essential tools to reach the SDGs. The Ambassador also emphasizes the importance of inclusivity in the process of shaping the digital age and invites all stakeholders, including civil society, private sector, academia, and technical communities, to share their perspectives.

Dr. Grienberger encourages the participants to share personal experiences and approaches on the topic with the other participants because this will make the consultations very rich in detail and in the perspectives that are shared and filter into the GDC. She points out the risks of the Internet – these days because of misinformation and disinformation, cybercrime, and scams – but encourages participants to also focus on the positive sides of the Internet: We can learn from global communities in a way that was not possible before the Internet was invented. Secondly, the Ambassador emphasized that, even though governments will sign the GDC, governments will not be able to shape the digital age as it is necessary. Therefore, all stakeholders - civil society, private sector, academia, and also the technical communities – are important and also present here in this consultation and are invited to share their perspectives, which will make the GDC become relevant in the end. Lastly, she highlights the necessity of cross-regional cooperation in shaping the Global Digital Compact as regional perspectives are highly significant to this global compact. Therefore, the consultation should focus on joint issues and common denominators for example digital commons, where India already is a champion, and the application of AI.

Dr. Grienberger highlights the interest in cross-regional cooperation in shaping the Global Digital Compact and encourages the discussion of joint issues and regional specificities. She points out that the consultations provide a valuable opportunity for a rich discussion on joint issues and regional specificities.

1.6 Ambassador Anna-Karin Eneström, Permanent Representative of Sweden to the UN

The Permanent Representative of Sweden to the United Nations, Ambassador Anna Karin Eneström, expresses gratitude towards the organizers and participants and shares about the process of leading the intergovernmental negotiations for the Global Digital Compact together with the Permanent Representative of Rwanda to the UN. The Ambassador states, that the GDC is a critical step towards enhancing global digital cooperation and achieving the Sustainable Development Goals. The consultations – including the regional consultations – conducted so far have been constructive and valuable, bringing in a wide variety of issues, including how digital tools can be used to boost the implementation of the 2030 Agenda and how to bridge the gender digital divide.

She encourages participation in the upcoming deep dives to be held from March to June by the co-facilitators Sweden and Rwanda. She further explains that an issue paper will be prepared after the deep dives and will be consulted with Member States in New York, feeding into the ministerial meeting in September.

Ambassador Eneström identifies eight areas that could serve as building blocks for the Global Digital Compact that are also reflected in the agenda for the Asia Consultation: digital inclusion and connectivity; internet governance; data protection; human rights online; digital trust and security;

artificial intelligence and other emerging technologies; global digital commons, and accelerating progress on Sustainable Development Goals.

The Ambassador emphasizes the importance of the regional consultations and their opportunity for all stakeholders to develop and shape a shared vision of digital cooperation. She states that the process is at a very early stage of the consultations and from the start the emphasis is on inclusivity, transparency, and meaningfulness. The Ambassador is happy to listen to the voices of the participants over the coming days and learn how they see challenges and opportunities in the digital transformation in Asia.

2. Workshop, Session, and Report Methodology

The workshop was the last of the three regional consultations. Like the two previous consultations, it aimed at acquiring opinions, inputs, and key messages to bring into the ‘Summit of the Future’ process. To do so, approximately 50 expert participants from various Asian countries were invited.

The Two-day workshop was preceded by a virtual preparation call for participants on 17 March 2023, clarifying its context, objectives, agenda, as well as the participants’ expectations and questions. From this day on, participants could also access a Miro board, a digital whiteboard, and real-time online collaboration tool, to access all necessary resources for the workshop: Recommended readings on the workshop’s topics, agenda, guiding questions for the different sessions, information on speakers and the GDC process. It also allowed participants to briefly present themselves and exchange contacts to stay in touch beyond the workshop.

The workshop itself was opened by the above-mentioned welcoming remarks, followed by an exercise to discover who is in the room and participates in the exchanges. As a result, it became clear that a balanced representation of governmental institutions, the private sector, non-governmental organizations, as well as academia and research, was assured. It also delivered transparency about which precise organizations were represented. In terms of participating age groups, about half of the participants were between 31 and 45 years old. Roughly one quarter of the participants also represented the group of 18 - 30 years and another quarter the group of 46 - 60 years. Only one participant was older than 60 years.

At the core of the workshop were 8 thematic sessions (sessions a - h), during which participants discussed and wrote down their input based on guiding questions. The guiding questions were not binding and participants could also address aspects not covered by those questions. Participants were also encouraged to focus on those questions to which they could contribute most or which were the most relevant ones for them. Each of the 8 thematic sessions was structured in a similar way based on the following sequencing:

- a) A short moment to reflect on the guiding questions by themselves (alone)
- b) A few minutes to exchange questions with a neighbor at the table (group of 2)
- c) A few minutes to exchange with another group of 2, sitting at the same table (group of 4). At this point, participants were encouraged to write down the ‘table-ideas’ on the digital Miro board.
- d) Between half and three-quarters of the session time was then dedicated to a moderated exchange in plenary, based on the discussions already started at the tables. Participants were asked to remain concise to allow a maximum of contributions.

New aspects that were brought up during the plenary were written down on the Miro board by two notetakers. Participants followed the notetaking of everyone on their own laptop and smartphone devices, as well as on the big conference screens provided by the venue so that there has been transparency about which aspects were written down and how they were formulated at any given time. The participants were also encouraged to underline or reinforce a statement on the Miro board by adding an exclamation mark icon to the note in question. They were equally encouraged to display their dissent regarding a taken note by adding a lightning icon to it.

After each session, the respective part of the Miro board was locked, so no further modifications could be made by any participants. There was, however, the possibility to add comments to the existing notes until the end of the event.

This report, including the final recommendations to the GDC, has been developed based on those contributions noted on the Miro board. Responsible for the first report draft were five ‘Report Champions’ who consisted mainly of workshop participants. This draft was then opened to be reviewed and approved by all workshop participants. In the following chapters, the detailed results from each thematic session, as well as condensed key messages per session, are displayed.

3. Work Session (a): Role of Digital Public Goods (DPG) including Digital Public Infrastructure (DPI) in the GDC to achieve the 2030 Agenda

3.1 How can emerging technologies and digital applications be used to address contemporary challenges?

A few important contemporary areas where emerging technology can help address challenges that the participants identified in their discussions, included Climate Change, Access to Healthcare and Finance, Agriculture, Education, and Social Welfare and Protection schemes. In addition, the role of emerging tech in decreasing corruption by weaving in trust transparency, and accountability was also stressed. The group used a broad definition of emerging technologies ranging from drones, AI, open data, and digital public goods and infrastructures each of which played crucial roles in the overall ability to respond to challenges. To do so emerging technologies needed to be thought of as supplementing but not substituting human capacities and resources when dealing with contemporary challenges.

The group also stressed on the need to adopt holistic and proactive approaches to emerging technologies and digital applications. While recognizing that currently emerging technologies are often used in an ad hoc manner to respond to a crisis, this mode of operating leads to solutions not being built bottom-up and taking into consideration all ecosystem actors. This meant that the potential of emerging technologies that lend themselves to customization to special needs and contexts was not harnessed effectively.

The group highlighted the importance of bringing in a level playing field by expanding access to emerging technologies to a wide swathe of the population across different contexts and realities. While emerging technologies can help elevate and bring people to the same strata to do so it is important to have more representative data from all quarters of society – especially children in developing countries. Such proactive and holistic approaches should acknowledge and respond to the gender gap, the accessibility gap, the urban-rural gap, the language gap, and structural issues of casteism, ableism, homophobia, transphobia, classism, and xenophobia which can easily be magnified in an online world. A proactive approach would also need to overcome the foundational challenges of infrastructure, literacy, and affordability.

The participants identified the importance of stakeholder engagement and consultation at the right levels to enable a bottoms-up approach to addressing these challenges and coming up with solutions that can be personalized and/or adaptable to different contexts.

Original comments on the Miro board during the session:

- Emerging technologies lend themselves to customization to special needs and contexts, however, we need to overcome the foundational challenges of infrastructure, literacy, and affordability.
- Transparency and accountability in governance: for instance, fruitful stakeholder discussions on draft laws are needed.
Disabilities and accessibilities
Employment and Equal opportunity
- Institute interoperability laws so that DPIs get actually used, and not just Bit-Tech provided infra.

- Emerging technologies are often used in an ad hoc manner to respond to a crisis, not building bottom up, taking into consideration all ecosystem actors.
- Affordable
- Supplement but not substitute human capacities and resources
 - Open data used for research in resolving climate change issues, measuring SDG indicators
 - Open source technologies to develop tools used in government and by the public
- Bring in the level playing field by expanding access to a wide set of the population from diff contexts and realities; emerging tech can help elevate and bring people to the same state
- to have more representative data from all quarters of society, especially children in developing countries- additionally, Emerging Tech must adhere to principles of data (Data commons)
- What are the contemporary challenges?
- Access to healthcare, and finance to those in remote areas: Drones used during Covid for vaccine delivery, AI test management rules for calculating agricultural product damage, blockchain used for calculating credit score regarding loan repayment by Self Help Groups.
- Personalised/adaptable solutions
- Reduce silos within governmental platforms
- to address the problem of scale and provide service delivery in public health, education, and social protection schemes
- Emerging Tech can help decrease corruption which is a rampant problem for the region by weaving in trust and transparency and accountability
- to address the problem of scale and provide service delivery in public health, education, and social protection schemes
- to break silos and to have interoperable data-data standards (data commons - data as a shared resource, as a DPG)
- important to acknowledge and respond to the gender gap, the accessibility gap, the urban-rural gap, the language gap, and structural issues of casteism, ableism, homophobia, transphobia, classism, and xenophobia which easily go online
- Emerging Technologies can be used in the climate crisis. Energy optimization and tracking carbon. It is means to an end using a bottom-up approach. Need to identify at which stage should the stakeholders be involved.

3.2 How can the GDC facilitate sharing of Digital Public Infrastructure and/or Digital Public Goods among Member States?

The participants felt that on some topics the GDC process could play a facilitative role including:

- Helping countries save costs and time and accelerate their efforts by making commonly needed digital public goods discoverable
- Enabling capacity building among civil servants and public officials by providing them with access to technical expertise, procurement guidance, and driving cross-country sharing of experiences using the UN system.
- Facilitating the setting and adoption of principles and standards for DPGs and DPIs that govern their creation and use, while safeguarding against new forms of rent-seeking within and between countries.
- Identifying DPIs that need to be developed at a global level and the institutional support needed to create these.
- Supporting the creation of appropriate funding pools and mechanisms to support the implementation of DPGs/DPIs. Such funding must be for the full lifecycle of DPI projects – and go beyond mere implementation.

Participants also felt that in some areas the GDC could have requirements that countries commit to the meeting including:

- Requiring relevant open data sets to be made available by governments as well as private companies that have received public investment at any point. These could also include data generated/held in DPIs.
- Requiring countries to make in principle commitments to open source and maintain SDG-relevant systems such as DPG/DPI.
- Putting in place the needed checks and balances – including relevant national/international institutional regimes – to prevent the abuse/misuse of DPG and DPI by member states. These should ensure the protection of end users.
- Addressing IP/ Proprietary issues through legal/regulatory mechanisms - so that stakeholders have assurance about their contribution to DPIs.

Original comments on the Miro board during the session:

- GDC should facilitate and reach some sense of agreement on what kind of Digital Infrastructure will constitute Digital Public Infrastructure.
- Cost saving, Time, Acceleration, best practice common platform with open source:
- Digital Identity, Payment Gateway, Mechanism to provide cheap/affordable computers, Online Public Service Template, Capacity Building.
- holding government and private companies (that at any point received public investment - e.g. telecom) to account for their data being open and accessible.
- GDC should facilitate the discussion on what kind of Global DPI can be developed at a global level and what level of institutional support is needed to move in that direction? (using the commons approach).
- GDC ensures continuous capacity building among civil servants/public officials who are implementing the GDC in the country.
- GDC should help build capacity for DPG development (DPGA is facing challenges)
- Promoting and setting standards for DPIs - open, safe, inclusive DPIs. Promoting Open Standards and Open Source; Interoperability; scalability and modular systems; privacy by design, avoiding vendor lock-in, etc.
- GDC could act as a knowledge management service (to avoid duplication) including capacity building and providing a network of expertise.
- Increase the community around DPGs to meet demand from member states
- Procurement guidance to member states to be able to work with DPGs, access technical expertise from outside the country/region.
- Ensuring that the data in the DPIs are open, with the ability to mine and meaning-making algorithms as private sources of competitive advantage.
- GDC includes a list of open data sets that should be made available by the governments.
- Support South-South Cooperation in sharing DPI/DPG experience, including using capacities and networks of the UN system.
- In principle commitments to open source and maintain SDG-relevant systems such as DPG/DPI.
- Avoid redundancy, build interoperability and democratic values: Using the mass-scale deployment of successful DPIs to build knowledge and design standards through a bottom - p approach that allows inclusivity accessibility and interoperability.

- GDC can help in standard setting - with lessons from vendor lock-ins.
- Replication of success between states/countries.
- Reconfiguration for replication will need appropriate funding.
- Hold member states accountable to open data.
- Need to make sure that DPI and DPG and the tech behind it are not abused/misused by member states themselves for eg. when conservative anti-rights regimes come to power - how to make sure that this does not get 'shared' as it has happened before.
- (Institutional regime at intergovernmental level keep checks and balance and guardrails)
- Develop principles for governance of DPIs towards fairness and equity, and disallowing new kinds of rent-seeking, and using code/ architecture as law in an illegitimate manner not subject to democratic processes.
- Building beyond the right DPI instead of replicating. Cooperation and corroboration between member states.
- IP/ Proprietary issues need to be addressed through legal/regulatory mechanisms - so that stakeholders have assurance about their contribution to DPIs.
- Funding must be for full lifecycle of DPI projects - beyond implementation. Should also factor in re-imagination, reconfiguration, and learning. Focus on design stage as well instead of just building.
- Actioning DPI interoperability by building local capacity with participation of universities, civil society.
- DPI and DPGs are different concepts. Must be addressed differently.
- Ensure the protection of end users.
- GDC must drive funding mechanisms v/s create new financing vehicles also new governance mechanisms.

3.3 How can DPIs promote innovation by the private sector including MSMEs and what constitutes the basic building blocks of DPIs?

The participants opined that innovation is not something to be owned or promoted. It should be a part of the culture around DPIs and DPGs. While thinking of DPIs it is useful to think of (a) technology and building blocks like identity, payments, data layers, logistics layers, access to credit layers, and service delivery layers, in addition to (b) governance building blocks like cyber security agreements, data trusts and (c) finance building blocks like government funds which can anchor seed/first loss funding for MSMEs.

New technologies provide great opportunities for startups and micro enterprises. New products can be set up at a fraction of previous costs, with automation and cost savings available for all. But education is needed on what is available to the ecosystem and how they can use it. India's example of the government building the digital backbone of DPI around which the private sector and others innovate has a lot to offer.

Original comments on the Miro board during the session:

- Innovation is not something to be owned or promoted. It should be a part of our culture around DPIs and DPGs.
- Tech Building Blocks: Identity (Tax Based), Payments, Logistics Layer, Access to Credit layer.
- Governance Building Blocks: Agreement on Cyber Security, Access to Data Trusts to unlock Credit, Business Intelligence.
- Finance Building Blocks: A Government Fund which can anchor seed / First Loss Funding for MSMEs.
- It comes down to educating youth and adults on how to use technology, including MSMEs.
- New technologies provide great opportunities for startups and micro enterprises. New products can be set up at a fraction of previous costs, automation, and cost saving available for all. But education is needed on what is available and how to use it.
- Creating a good business model to encourage the private sector to participate in the DPI ecosystem.
- India's example of building the digital backbone of DPI around which the private sector and others innovate has a lot to offer.

3.4 What level of contribution is expected from stakeholders to build sustainable economic development models using digital technologies?

All participants emphasized the need to create an enabling policy and legislative environment in countries to address areas such as transparency and accountability in the governance of emerging technologies and the need for fruitful stakeholder discussions on draft laws. This also included the need to include provisions to address factors such as disabilities and accessibilities; employment and equal opportunity. One key suggestion was to ensure draft laws were posted in accessible online locations for broader public consultation and comment.

At a more technical level, the group highlighted the need to institute interoperability laws so that DPIs get used. This would also serve to address the issue of reducing siloes – especially within governmental platforms – and to have interoperable data supported by data standards to create data commons as a digital public good.

Participants suggested that to promote responsible and sustainable development of digital technology, Ministries of Education and innovation hubs should embed Principles of Digital Development in their activities. The states should ensure equal opportunities for everyone in digitalization, policy and regulation adoption, and more resources for digital public goods. The design of Digital Public Goods and Digital Public Infrastructure should prioritize privacy, transparency, and accessibility, and should be open to assessment by independent actors. Private sector actors leveraging DPGs and DPIs should contribute back to their maintenance and development by establishing OSPOs, and sustainability should be viewed beyond financial sustainability. Finally, there must be transparent procurement systems where procurement datasets are made public.

Original comments on the Miro board during the session:

- Ministry of Education / education programmes or innovation hubs should be embedding Principles of Digital Development in all aspects of creating technology
- Development Partner

- a. Constant reminder to government to follow international commitment/ standard/ treaties
- b. Equal opportunity for everyone in digitalization Government
- c. Policy and regulation adoption
- d. More resources to adopt digital public goods
- e. Interoperability, Compatibilities, and Compliance Private Sector
- f. Public Private Partnership for sustainability.
- Design of DPG and DPI needs to be rights-based - privacy by design, transparency by design, accessible by design. Design should be localisable, not set in stone, and iterative. DPI and DPG should be open to assessment by independent actors.
- Encourage Private sector actors leveraging DPGs and DPIs to contribute back to their maintenance and development by establishing OSPOs.
- Sustainability should be viewed beyond financial sustainability.
- Transparent procurement systems where procurement datasets are made public.

3.5 How can the global development community channel dedicated funding for the development of a DPI ecosystem?

Developing a DPI ecosystem requires addressing a range of issues regarding funding and sustainability models. These include:

- Thinking beyond the initial implementation - along with solving the problem of initial capital to establish a DPI, funding must also be considered from the lens of maintaining the DPIs. If DPIs can have self-sustainable business models that are not continuously reliant on grants or public funding, then countries could potentially apply project finance approaches that have been useful to solve other kinds of infrastructure funding challenges.
- At a global level, the creation of a dedicated funding and coordination facility to align MDB programming to DPG/DPI approaches can be explored similar to how the Global Financing Facility for Health aligns different large-scale funders.
 - Preventing redundant effort by streamlining funding to support replication and reuse of proven DPG and DPIs
 - Promote investment approaches that create incentives for system-wide investments and not just sector-specific silos
- It is also important to invest in developing regional centers of excellence and networking them to develop in continent capacities to seed and grow the DPI ecosystem.
- Funding for DPIs, like funding for other infrastructure, needs to be consultative with the public. The reason for the usage of the public pool needs to be transparent, accountable, and open to critique and oversight.

Original comments on the Miro board during the session:

Along with the problem of initial capital, funding must also be considered from the lens of maintaining the DPIs. Hence identifying some good revenue models alongside the sources of funding - Can we apply project finance approaches?

- It starts with solutions that have a self-sustainable business model, as not all solutions in the DPI ecosystem should be continuously reliant on grants or public funding. There is also potential for quadratic funding - based on a number of funders rather than the amounts based on single funders.
- Create a dedicated funding and coordination facility to align development community programming to DPG/DPI approaches
- Invest in developing regional centers of excellence and networking them to develop in continent capacities.

- Funding for DPIs, like funding for other infrastructure, need to be consultative with the public – esp. the most structurally vulnerable groups. The reason for the usage of the public pool needs to be transparent, accountable, and open to critique and oversight.
- Prevent replication of effort (and associated redundant funding that can be better leveraged elsewhere) by streamlining funding.
- funding to support capacity development as part of key foundation for success of DPIs.
- funding that creates incentives for system-wide investments and not sector-specific silos.

3.6 How can DPIs and digital technologies be used for the development of low- and middle-income countries?

DPIs can provide scale - hence an opportunity for low- and middle-income countries to leapfrog the development curves. To do this accessibility and teachability need to be a part of how DPIs are conceptualized. There needs to be a concerted effort to engage and support co-ops and civil society organizations to use DPIs and DPGs as part of their work. It is also important to not treat DPIs as homogenous and customize their application to local needs and values

DPGs and DPIs should be used to generate and collate development-related indicators that can be published as a part of national statistics. It is also important to keep in mind that solutions developed in LMICs should not be restricted to LMIC contexts alone and global cooperation for their adoption should be pursued.

Original comments on the Miro board during the session:

- DPIs have the ability to provide scale - hence an opportunity for low and middle-income countries to leapfrog.
- Accessibility and teachability need to be a part of DPIs and tech. Development cannot happen without this.
- Support co-ops and civil society organizations to use DPIs and DPGs as well as build the bridges needed.
- Intersectionality is important to include structurally silenced groups eg. women, oppressed castes, PwDs, etc. in developing access and knowledge around this.
- Solutions developed in LMICs cannot be restricted to LMIC context and global cooperation may be required for global adoption.
- Not treating DPIs as a homogenous block and customizing the application of DPIs to local needs keeping in mind the local values.
- Being able to use data exchange on a platform as a mechanism.
- Open Source Technologies
- DPIs and DPGs shouldn't necessarily be used synonymously - although there cannot be DPI without DPGs, as it would be called Digital Proprietary Infrastructure.
- Startups in emerging markets can now leapfrog using the new technologies, and the barriers to market entry are reduced as is greater access to global customers.
- DPIs and DPGs shouldn't necessarily be used synonymously.
- Use DPGs and DPIs to generate/collate development-related indicators and publish them as part of national statistics.
- By building capacities of govt. in low and middle-income countries.
- Capacity building of last-mile service delivery.

4. Work Session (b): Inclusive, open, accessible, safe, and affordable digital technologies and infrastructure and their co-governance

4.1 What is the role of stakeholders in ensuring inclusive, open, accessible, safe, and affordable digital technologies?

The focus was on the roles of the Government and the private sector.

The Government should formulate Digital Inclusion policies on infrastructure for Internet coverage in the entire country, establish regulations for open sources and interoperability between the Government and the private sector, create incentives for unconnected regions (USO), implement the taxation of the digital sector, ensure lower tariff of imported equipment, provide digital capacity building for citizens, ensure privacy and data protection, and ensure the protection of children's rights and safety.

It should also provide a minimum level playing field and address areas of market failure. Another role would be to develop nationwide identifiers and ensure the classifications of information, controlling the dissemination of unsafe or dangerous information.

Instead of supplying digital goods/services/infrastructure which are well provided by private companies, the Government should focus on regulating safety and competition. Besides, the Government should ensure active community outreach and solutions seeking for needs, not vice-versa.

The private sector should invest in local content/platforms. Local players should be viewed as co-creators of new local markets instead of threats to high-priced spectrum. Companies should apply the human-centered approach and the universal design in every product /service to ensure accessibility for all, including people with disabilities, by engaging different user groups in all stages of the decision-making process and making sure their voices are heard.

Original comments on the Miro board during the session:

- To formulate Digital Inclusion Policy addressing: infrastructure for full coverage in the country, regulations for interoperability between government and private sector, incentive for unconnected region (USO) and lower tariff of imported equipment, building trust for citizens, capacity building for digital adoption.
- Govt/ policymakers to ensure that children's rights and safety are protected.
- Active outreach to communities and shaping solutions to needs, not vice-versa.
- An important category of safety is AI running engagement algos with a commercial incentive, but are harmful to users, such as social media addiction. Children are particularly vulnerable - Government interventions on the creation of algorithms - i.e., engagement algorithms ->addiction
- Efforts should be on open source, not having vendor lock-in, and enabling interoperability.
- Pvt. sector: invest in local content/platforms: Private sector should view local players as partners - to build new markets.
- Govts should get out of provisioning digital goods/services/infra that is well provided by private capital. Instead, focus on regulating safety and competition
- Govt and lawmakers to ensure that access to the internet is by default privacy preserving & data protection.

- human-centric design in every design stage especially considering inclusivity of people with disabilities.
- The understated role of communities in helping the last mile get on to the digital world (adoption and empowerment of the "un-networked").
- The private sector has its own incentive to make products as accessible as possible, often for free. The constraint becomes digital infrastructure within countries
- Important to prioritize the factors.
- Stakeholder mapping should have two buckets: 1) A market-based system with price determination set by the market 2) A citizen-state interaction with capped markets and licensing
- For the government to be able to provide a minimum level playing field and address areas of market failure
- Govts to rationalize digital sector taxation (currently treated as a demerit good by high sector specific taxation)
- Govts to change policy to improve competitiveness of each part of the digital connectivity value chain (int'l bandwidth, backhaul, last mile) and to avoid monopoly.
- focus on open source/sharable content/knowledge.
- Even multistakeholder governance mechanisms need to be held accountable.
- Govt/policymakers: strengthen laws to track, prevent, and punish child abuse and exploitation enabled by technology.
- Global or Nationwide identifier - Classifications of information/control of unsafe/dangerous information being disseminated.
- Govt to Streamline access to rights of way and public sector connectivity infrastructure.
- DPI should not be created without the participation of youth, not only in consultations but in decision-making roles - without young people they cannot be sustained, they are also the users of the future, are we designing with the users in mind, do we even know what they want or need?
- Technology organizations - constitute multidisciplinary advisory panels for dpg/dpi roadmaps.
- Involving marginalized communities that could be impacted by digital tech - UN ensures the voices of the most marginalized heard.
- Role of government must be re-imagined due to govt. paternalizing factor.
- Finance - take a long-term view of the financing requirements - sustainability should be viewed through two lens (impact (SROI) and financial) - do not sacrifice impact for financial.
- Understanding the contours of accessibility is a must to weave inclusivity in tech and related infra – whom are we building for – defining the who is important before we get to the what and how stage. The base should not be limited to known categories and dimensions such as gender but also include categories of linguistics, cultural, and socio-economic realities. The metric to gauge accessibility is the diff ‘who’ can control the tech and what is the ease with which they can access redressal mechanisms.
- DPI governance to include a dedicated panel overseeing incidents of abuse/harassment - also to run periodic scenarios on how the DPI can be abused and strengthen response plans for different scenarios.
- Pvt Sector - View community networks as a partner who creates a market for you instead of a threat to your high-priced spectrum.

4.2 Which short-term measures are necessary and how can the GDC address this?

Rights enhancing, innovation-enabling, economically empowering, socially, and peacefully connecting digital use are the ultimate goals of inclusive, open, accessible, safe, and affordable digital technologies. To move towards those goals, the following short-term measures should be taken:

- Identify who are excluded: Women, people of lower economic classes, oppressed castes, LGBTQ, etc.
- Tradeoffs must be managed: safety, affordability, and accessibility are linked to inclusivity: often the same vulnerable and marginalized groups have to deal with the tradeoffs.
- Capacity building for meaningful engagement of stakeholders who may have little awareness.
- Establish governance mechanisms advisory and safety panels before systems go live. for existing DPIs /country's implementation, strengthen governance mechanisms where missing and/or deficient.
 - Facilitate the Digital Infrastructure and DPG.
 - Promote Digital Cooperation between Countries
 - Each state should sign up for the Marrakesh Treaty and create DPIs-related voice-to-text and voice that works for ALL languages.
 - Develop mainstream technology with assistive technology in mind. The best solution is an inclusive design, which meets the accessibility needs of diverse users.
 - GDC needs to develop a rights-based framework of unconditional openness, accessibility, and non-discrimination.
 - Definitions in technology are evolving - what is safe today could become unsafe tomorrow. GDC can facilitate consultations on those definitions.
 - GDC should promote freedom of expression

Comments on the Miro board during the session (edited for clarity):

- Inclusive doesn't mean only the people but also being inclusive by allowing for movements, social solidarity, critique of power. When talking about inclusivity, it's important to name who is being excluded. Women, people of lower economic classes, oppressed castes, LGBTQ, etc.
- Affordability and inclusion is located within the market/private paradigm. GDC needs to go into a framework of rights and openness which non-excludable and accessible unconditionally as well
- When so many fundamental rights are hinged on access to digital spaces and tech, GDC needs to ensure unconditional, inclusive.
- 'Openness' as a part of equity and autonomy - including bodily autonomy, agency, etc.
- 1. Facilitate the Digital Infrastructure and DPG, 2. Promote Digital Cooperation between Countries.
- Inclusive means maximizing the internet's public value.
- Mainstream tech v/s assisted tech for people with disability. Assisted tech can't keep up with mainstream tech. It is more expensive. Research should be taken into consideration while working on such an aspect.
- Safety as a universal concept that cuts across - safety not just for humans but across ecosystems - Sustainable models.
- For upcoming DPIs - establish governance mechanisms advisory and safety panels before systems go live.
- For existing DPIs - countries implement/strengthen governance mechanisms where missing and/or deficient.

- Trade-offs must be managed: safety and affordability; accessibility and safety. Linked to inclusivity: often the same vulnerable and marginalized groups have to deal with the trade-offs.
- Changing and evolving definition of technology -What is safe today could become unsafe tomorrow. GDC can help in managing these types of consultations.
- Frameworks/modules for meaningful engagement/education of stakeholders who may have little awareness.
- Sign up to the Marrakesh Treaty and create DPIs related voice to text and voice versa that work for ALL languages.
- "Safe" internet is not the goal. Rights enhancing, innovation enabling, economically empowering, socially & peacefully connecting digital use is the aim.
- Freedom of expression issues to be included in the GDC.

4.3 How can emerging technologies and digital applications be used to address contemporary challenges?

Participants highlighted that among the most common constraints figure language, knowledge, and low income. Furthermore, the current unsaid/implied market-centric/profit-centric way of approaching digital tech and the internet is a big constraint. Accessibility solutions may not be viewed by investors as scalable, but necessary solutions. Each digital product/service should meet accessibility standards and be experienced with different senses and be intuitive for all users. The development process should not merely tick the boxes. Technology should be designed with the participation of different groups in society (technologists, psychologists, anthropologists, PwD, less represented sections, etc.). Suppliers should value People over profit and offer products and services which are also affordable for poorer groups of users (including businesses and individuals).

Participants also stated that innovation cannot be just for the sake of innovation. It must contribute towards human rights and a safe, inclusive, open, and accessible society. Not everyone can take up new technologies so easily. Therefore, a little assistance from the state is needed. Lastly, there is also the issue of collecting information from citizens and profiling them and citizens giving up privacy/personal data.

Original comments on the Miro board during the session:

- Language accessibility being able to convert technological solutions.
- Diversity impacts the solution scape. Local contextualization is important
- language; knowledge; low income.
- The current unsaid/implied market-centric/profit-centric way of approaching digital tech and internet is a big constraint.
- Accessibility - Literacy of users - can we design on speech or visual images?
- Affordability for poorer groups of users (including businesses and individuals).
- Accessibility solutions may not be viewed by investors as scalable, but are necessary solutions. Can the public sector step in and invest?
- People over profit.
- Not accessible - not connected to the internet.
- Education/visibility on other types of technological solutions that meet these points.
- Innovation cannot be just for the sake of innovation. It has to contribute towards human rights and a safe, inclusive, open, accessible, 'affordable' etc.
- Digital is good but not everyone can take new technologies so easily, so a little assistance from the state is needed specifically on technical assistance.

- Certain govts have less power/control on social media platforms = hate speech, disinformation; More power/control = loss of freedom of expression, surveillance.
- The dilemma of collecting information from citizens to understand them vs citizens giving up privacy/personal data.
- Digital development teams should be multi-faceted so that there is inclusion and safety by design (technologists, psychologists, anthropologists, PwD, less represented sections, etc.).
- Lack of skills to program for people with disabilities.
- Technology by Design. Also, design technology with more representation from different aspects of society. Be more inclusive rather than mere check boxes.
- The need to recognize what the end goal is.
- Technology developers and designers must become more inclusive - this ties with education imparted to technologists not being holistic (broad worldview) in the first place.

5. Work Session (c): Co-Governance model for developing Global Digital Cooperation with trust, security, and resilience

5.1 What kind of cooperation and collaboration is suitable for ensuring trust, security, stability, and resilience in digital technologies?

The participants discussed the importance of establishing common principles when shaping the co-governance model such as building trust and accountability in the model itself while reflecting the beneficiaries in the creation of technology. The discussion touched upon the importance of strengthening existing mechanisms within the ITU and UN and upholding the role of legitimate public authorities in their governance role. The significance of trust as a basis of collaboration was stressed with a recognition that sometimes the very act of collaboration itself builds trust. Participants also recognized the importance of involving beneficiaries and those involved in the implementation a greater say in the design of technology. Some participants urged caution in both the use of Big Tech and the need for governance of Big Tech.

Original comments on the Miro board during the session:

- Transparency and accountability are important during the shaping of the co-governance model.
- Strengthen existing mechanisms within ITU and UN and scale them in structural supported by GDC to regional and country.
- We should share with the governments about the strategy of Global Digital Cooperation and ask for their feedback.
- Ironically trust becomes the basis for cooperation and often this is missing. V/S Sometimes states are forced to collaborate, this can foster trust.
- Co-governance is needed in which context the tech is developed. v/s "multistakeholderism" is a problem. v/s doesn't mean all stakeholders have an equal role. Big tech should be used with caution.
- Interoperability is a common notion between private and public goods.
- How do we build governance models that reflect the beneficiaries in the creation of technology.
- Giving implementors and beneficiaries voting rights on the design of the technology including prioritization of features, rather than the funders - DAO model.
- Need for a flexible system but not a changeable system. Need to find a third body to oversee the system.
- Different needs for private and public goods. Notions for accountability changes. v/s govt. must negotiate on behalf of citizens even if it is a private sector good.
- Speak like co-governance and multistakeholderism should have clear meaning and context, and not upend legitimate public authorities from their legitimate governance role. Big Tech is getting too much 'governance' role in digital governance while they are the ones most in the need of governance. This problem should be addressed systematically.

5.2 How can the GDC contribute to developing global digital cooperation?

According to the participants, the GDC can develop procedures for legitimate cross-border data transfer for government purposes and focus on the internet as a public good. Participants also agreed that the GDC could define standards for a safe and trustworthy internet, and address data localization resulting from a lack of trust. It is also important to push back against anti-democratic, anti-gender, and profit-driven uses of technology.

Participants also suggested that the GDC could be institutionalized within a dedicated organization to facilitate global digital cooperation continuously. Furthermore, it was seen as an occasion to strengthen existing forums.

Original comments on the Miro board during the session:

- Develop procedures for cross-border data transfer for LEGITIMATE needs of governments (e.g. regulating financial crime) beyond the Budapest Convention.
- Internet is a public good. This needs to be a core value to push cooperation
- Dedicated organization in charge of GDC to facilitate the global digital cooperation
- Using the GDC to strengthen existing fora (ICANN, IGF, WSIS, G20, WEF) and building inter-platform cooperation instead of institutionalizing a new mechanism.
- Existential Assumption was that the GDC was for global digital cooperation. To hear how it can contribute towards cooperation is a bit foundation shaking.
- To center internet as a public good, important to push back against anti-democracy anti-gender profiteering via technology.
- Define standards on what is a safe, accessible, trustworthy internet for both govts and cooperations should follow?
- Cross border data flows. There is data localization due to a lack of trust.

5.3 What kind of cooperation and collaboration is suitable for ensuring trust, security, stability, and resilience in digital technologies?

Participants highlighted the likelihood of technical standards on accessibility, language, etc to be effective when implemented in steps and starting with the government. The discussion also touched upon the need for ensuring that essential services could be accessed across the digital divide. Shared global challenges like climate change that need coordinated global action both need and can be the impetus for establishing regulations and standards, as well as systemic drivers like e-commerce and cross-border data flows. The participants reinforced the need for such regulations and standards processes to engage the relevant stakeholders including experts, citizens, and end users. Finally, the role of technical standards and certifications in facilitating the creation of a global talent pool and enabling cross-border labor mobility was also stressed.

Original comments on the Miro board during the session:

- Creating a global talent pool and enabling cross-border labour mobility.
- Challenges that require coordinated global action - eg: Climate action.
- Regulation and technical standards on accessibility, language, etc. may work more when implemented in steps, starting with the govt.
- An informed policy approach that enables the framing of effective techno-legal regulation by facilitating a dialogue between public technology and public policy experts to come together- to shape market behavior and frame optimal governance frameworks for new-age digital technologies.
- E-Commerce and Cross Border Data Flow.
- Essential services should not be digital-only. There must be alternative pathways.
- Prerequisites to prove responsibility and inclusion for building high-risk applications.
- With global consumer trends, where there is globalization of music, and entertainment, there is a need for global standards of consumer data.
- What we are using technology for - it's not a silver bullet. Standardise asking people what they want.

- Weigh the benefits of opt-in vs opt-out models for different services.
- That which impacts globally - such as data flows; usage etc or use of emerging tech.
- Government procurement contract models and procurement information to monitor.

6. Work Session (d): Inclusion and Gender Equality in global digital transformation

6.1 How can we ensure inclusive participation?

To ensure inclusive participation, first and foremost, a correct understanding of gender identities and diversity is essential. Gender is a spectrum, including men, women, and non-binary. Gender should not be a “niche” topic. Diversity covers all ages, ethnicity, gender, disability, caste, race, and religion groups. Therefore, the representation of diverse groups should be ensured, so meaningful participation of the most marginalized and intersectional vulnerable groups takes place. Tech design should be sensitive to their needs, ensure their access to the grievance mechanisms and have meaningful control over their data.

Furthermore, all digital platforms must be accessible to all. This can be achieved by consulting with representatives of diverse groups of beneficiaries – from the design to the evaluation stage. Their voices should be reflected in the decision-making process. It is necessary to identify potential barriers to participation, such as lack of access to technology, limited digital literacy or skills, language barriers, behavioral or cultural, or social biases, and figure out appropriate solutions.

Participants also recognized that exclusion in digital lies in exclusion in analog aspects (income, education, jobs, etc). So, some solutions are long-term (other can be short-term), such as creating feedback mechanisms in partnership with organizations that work with disadvantaged/excluded groups to create feedback loops into programs and processes; enhancing diversity in employment at tech companies and enrolment in university courses /scholarships; open the contribution process to certifications on what products are safe and products that are produced. For example, the DPG Standard is open in itself, where many people can help contribute and discuss the DPG Standard.

Original comments on the Miro board during the session:

- Gender is not just man or woman.
- Diversities apart from gender because of intersectionality - women and gender-diverse persons in all their diversities - caste, class, and race.
- Inclusive participation in policy spaces, tech design, usage, etc. with meaningful representation.
- Let's Think beyond binaries in gender.
- Ensure that all digital platforms are accessible for all.
- Consultation with representatives of diverse groups should be done from the designs to the evaluations.
- Ensure meaningful participation of the most marginalized and intersectional vulnerable groups.
- Beneficiaries should be included in the consultation and have a seat in the decision-making process.
- Multi stakeholder's process involvement in digital development
- It is necessary to identify potential barriers to participation, such as lack of access to technology, limited digital literacy or skills, language barriers, behavioral or cultural, or social biases.
- Gender should not be a “niche” topic.
- Recognize that exclusion in digital lies in exclusion in analog aspects (income, education, jobs, etc). So some solutions are long-term (others can be short-term).
- Create feedback mechanisms in partnership with organizations that work with disadvantaged/excluded groups to create feedback loops into programs and processes.

- Diverse hiring policies in tech companies and diverse student recruiting policies in university courses/scholarships.
- India's growing digital footprint includes a lot of young inexperienced vulnerable and marginalised sections, tech design should be sensitive to their needs and wants to ensure access to the tech and grievance mechanisms and meaningful control over their data.
- Have multiple gender representations while designing - "Inclusion by design".
- Don't use big words.
- Open the contribution process to certifications on what products are safe and products that are produced - for example the DPG Standard is open in itself, where many people can help contribute and discuss the DPG Standard.

6.2 How can bridge the digital gender divide?

Participants suggested restructuring how we understand inclusion and that it should be considered and embedded in the starting point of every digital undertaking. The "gatekeeping" mindset towards women should be transformed and issues of gender and social institutional discrimination addressed.

Participants were also in favor of applying the intersectional gender approach to access and the application of human rights online, with specific attention to online gender-based violence and gendered disinformation.

Some practical steps that can be made would be to address education from the school years so that women are both exposed and incentivized to participate in the digital world which would also allow for a higher number of Girls in the Tech / STEM field right from the beginning. Women should also be brought into the tech design processes. Women in tech should also easily have access to childcare benefits and maternity leave.

Other practical suggestions included building tech that enables women to hide their online activity when they share someone else's phone or the use AI to identify non-consensual intimate images and build in layers of consent before allowing publication on content platforms/social media.

Participants pointed out that the increase in AI technology means that employability is driven by human intelligence skills such as empathy. It could be seen these skills are more feminine, which in itself bridges the digital gender gap.

Original comments on the Miro board during the session:

- An intersectional gender approach to access and the application of human rights online, with specific attention to online gender-based violence and gendered disinformation.
- Medium term - Build tech that enables women to hide their online activity when they share someone else's phone.
- Use AI to identify non-consensual intimate images and build in layers of consent before allowing publication on content platforms/social media.
- Restructure how we understand inclusion. Language of inclusion is itself secondary. Needs to be from the start.
- Gender Obsolescence
- More Girls in Tech / STEM right from the beginning.
- Building analog foundations first.
- Contextual engagement. Blanket rules can do more harm than good.
- Work on changing the "gatekeeping" mindset toward women.
- Address issues of gender and social institutional discrimination.

- Decision-making groups and panels and anyone upskilling, creating, developing and implementing solutions should take into account of gender-equality - NO MANELS (No all male panels).
- The increase in AI technology means that employability is driven by human intelligence skills such as empathy. It could be seen these skills are more feminine, which in itself bridges the digital gender gap.
- Work bottom-up - identify community champions.
- Gender-sensitive data collection and gender-disaggregated data publication (data related to the digital).
- Use tech to combat crimes.
- Cover diversity groups.
- Short-term solution - Bring women into the tech design process.
- Child care benefits, maternity leave for women in tech.
- Short-term solution - Women sales agents at phone hops.
- Address education from the school years so that women are both exposed and incentivized to participate in the digital world.

6.3 How can risks and challenges such as gender-based online violence be addressed?

Participants highlighted that the focus should be on changing men's behavior and mindset as perpetrators of violence and not those of women or excluding them from / limiting them in online spaces. Another solution could be to conceptualize and operate cybersecurity that is centered on people and their rights and experiences. It would also help to build alliances to increase the voices to talk and work with Big Tech/Social Media to counteract Online Gender-Based Violence.

Another point of entry would be to enhance digital safety training by design. The core issues behind OGBV need to be addressed, too, and legal procedures to criminalize GBV should be strong, clear, and accessible in the public domain. Increasing the participation from grassroots level e.g. religious communities, rural communities, and schools will be important to effectively address OGBV. Participants also agreed that there need to be safe spaces to discuss experiences and perspectives stigma-free.

Original comments on the Miro board during the session:

- A conceptualization and operationalization of cybersecurity that is centered on people and their rights and experiences.
- Focus on men and/or perpetrators of violence. Change THEIR hearts and minds.
- Gender and tech is not just violence. I want to be present, not just safe.
- Pleasure, community, publicness, fun (solidarity model).
- Accountability from platforms and state.
- OGBV continues coz its profitability.
- Gender-based online violence is an accessibility issue. Harassment leads to vulnerable groups leaving platforms
- Enhance digital safety training by design
- Building alliances to increase voice to talk and work with Big Tech/Social Media M to counteract Online Gender-Based Violence.
- Do read the Prajwala Order of 27.10.2017.
- Core issues behind OGBV need to be addressed.
- Train AI models to crawl social media and automate moderation of public forums.
- Legal procedures to criminalize GBV - strong, clear, and accessible in public domain.
- gender-sensitive digital literacy capacity building!

- Increase participation from grassroots level e.g., religious communities, rural communities, schools.
- Safe spaces to discuss stigma-free.

6.4 How can we increase/ensure digital literacy, awareness, and skills?

The actions suggested by participants include raising awareness among governments about the importance of digital accessibility for marginalized groups, ensuring affordable digital devices, conduct technological capacity building for CSOs to transfer digital skills to end-users. It would also be important to allocate the state budget for digital facilities for marginalized groups, mandate minimum digital literacy training for all working groups, include access to sexuality, SRHR, abortion, and gender identity education in digital literacy online, and make it part of the school curriculum within K-8 grades to address digital literacy divides.

Original comments on the Miro board during the session:

- CSW67 Conclusions have good language on this (needs to be more gender diverse inclusive).
- Digital literacy online needs to include access to sexuality, SRHR, abortion, gender identity education.
- Need to address the unpaid labor done by women in tech - skills that are present are unacknowledged/uncredited.
- First, connectivity to the internet must be addressed.
- Ensure affordable digital devices.
- Conductivity for CSO, so that they can offer digital skills for end-users, the most marginalized groups.
- Address digital literacy divides.
- Allocate the state budget for sufficient digital facility for marginalized groups.
- Provide device-agnostic services; not overly dependent on apps - like what emails are. accessible on even a public/shared computers.
- Aware-raising for the governments about the importance of digital accessibility for the most marginalized groups.
- Private sector has a part to play when it comes to education and upskilling their workers on digital literacy.
- Mandate minimum digital literacy training for all working groups.
- Let's avoid preaching whilst communicating.
- make it part of school curriculum within K-8 grades.

Day 2, March 22 2023

**Global Digital
Compact
Consultations**



7. Work Session (e): Impact of artificial intelligence, machine learning, and emerging technologies on online/offline privacy and protection

7.1 What are the risks associated with AI, ML, and other disruptive technologies to online/offline privacy?

Participants felt that the key risks associated with AI, ML, and other disruptive technologies to online/offline privacy and protection are misuse of one's personal data, or images without their consent for harmful or commercial reasons; unfair treatment of certain groups caused due to biases introduced by inadequately trained AI models leading to online/offline privacy risks; intentionally spreading misinformation that is potentially damaging to individuals or business competitors by either hacking or manipulating the AI models; excluding or rejecting services because of biases/stereotyping; and mishandling of personal and sensitive information leading to identity theft or financial fraud. Participants also discussed the pronounced risks to children's privacy and safety when AI influences their online choices of content and friends because children often lack the agency and resources to respond to biases or misinformation.

Original comments on the Miro board during the session:

- Deepfakes and the creation of images of one's likeness without one's consent
- As they become more sophisticated, AI and ML algorithms may be able to collect, analyze, and use vast amounts of personal data without individuals' consent or knowledge.
- AI combined with an internet business model is a risk (algorithms trained for virality).
- Risk of over-reliance on AI models for social network moderation instead of human moderation. Risk is pronounced for local/regional contexts.
- Children are already interacting with AI technologies. Algorithms provide recommendations to children on what videos to watch next, what news to read, what music to listen to, and who to be friends with. Children lack the agency to fully understand the implications of AI technologies and often do not have the opportunities to communicate their opinions, nor the right advocates to support them.
- Go beyond risks for privacy; other risks are: copyright, blackbox going rogue.
- Some people can make some bad information and do harm to their competitors via AI since AI uses online information to make decisions.
- Consumers in the mainstream do not understand what the risks associated to utilizing emerging technologies - do the young generation understand what the risks are, there's so much built-up excitement but in the consumer space, they're not educated on how this would affect them and the risks.
- Train AI with public data, but AI model is not public good.
- Risk of inaccessibility.
- Accessibility in the afterthought.
- There needs to be more focus on distributional issues vis a vis AI, with AI becoming by far the biggest economic force .. who gains, who loses, who owns and controls, and who just consumes?
- Interaction between AI and data should be on digital public infrastructure, so it is both safe and fair to all.
- No transparency on the backend/ coding/ system of AI.
- Consider looking at Cross usage of tech in designing risk management – for instance, while AI is known for its exclusion risks, blockchain is touted to embed trust and transparency – within an ecosystem, can we look at marrying emerging tech to solve the issues they create.
- People in developing countries are left behind AI.

- Least of connection with diverse groups of end-users including persons with disabilities.
- Outdated hardware, especially for the poor.
- Algorithmic biases in ML systems run the risk of marginalizing those already marginalized.
- Training datasets when biased, bias the ML system.
- Also needs AI to be 'fair by design'.
- Future of Jobs: 65 percent of students starting elementary school today will eventually work in jobs that don't exist. What skills do young people need and how can we ensure we provide them through formal education and other pathways?
- Education in AI must be addressed. Future jobs will be different due to AI.
- Risk of ignoring current context most AI/ML learns from historic data. Concentration of knowledge since the larger population undergoes a learning curve that might prove unfair
- Gap in access to AI, ML, and other disruptive technologies in developing countries
- Good actors are centralized, bad actors are decentralized.
- Exclusion is a risk (not being counted and served by AI systems). Not just privacy
- Inherent human biases can make it into AI models when training and datasets are not carefully crafted to address bias in itself – e.g.: representativeness of population in visual databases/human biases in decision-making getting trained into models.
- Privacy is a very narrow framing.
- The gamut of AI is much broader and far-reaching.

7.2 How can AI and ML be used to identify and fight against misinformation and disinformation which may be generated by AI and ML?

Participants broadly discussed measures in three areas to combat misinformation generated by AI / ML: (i) Regulatory measures such as responsible usage licenses, setting standards for design, development, use, management, audits, and evaluation of emerging technologies, the inclusion of child rights and interests in all aforementioned standards, and constitution of governance bodies with defined roles and accountability at State or Global levels to exercise the regulatory measures; (ii) using Good AI and integration with other emerging tech models to build credible and accountable systems that can detect and arrest the spread of misinformation or have risk mitigation mechanisms; (iii) AI-enabled AI / ML literacy for end users.

Original comments on the Miro board during the session:

- Institute responsible use licenses for generative AI.
- NLP to identify misinformation is already done. But language and data resources are hard to develop (funding and open data).
- Global trusted AI and ML Engine to detect misinformation and disinformation.
- By analyzing patterns and trends in online content, AI can help to identify false or misleading information and prevent it from spreading.
- Good AI to fight bad AI, a never-ending race.
- The regulation of AI must be in favor of humanity.
- Consensus mechanism to adopt standard and audit algorithms for AI, ML.
- State must regulate AI at the international level.
- AI literacy - train more people to access it.
- Require audibility of algorithms when used in public systems and/or public influencing roles (SM/News).
- Privacy by design.
- AI as a living element of the society.

- There should be a regulatory body in Global level to audit AI and ML. New and emerging tech moves faster than regulations can catch up - use cases come up first. Future use cases may be regulated first.
- Speed the reactive risk management learnings to develop a robust proactive risk mitigation technique/s.
- AI is a paradigm, not just a tool.
- AI cannot be a silver bullet.
- IMP to say what AI, ML can address and where human intervention is required.
- Marrying AI and ML with other emerging tech like blockchain could be explored for its potential to embed trust and transparency and accountability in the ecosystem.

7.3 How can emerging technologies be used to protect against online crimes?

Participants discussed that emerging technologies could be used as the first level of protection to automate the continuous online scanning, detection, and flagging of fraud, hate speech, violations of standards or codes, etc. which can then be subjected to human review and adjudication. Emerging technologies could also predict or recognize the possibility of harmful behaviors, such as cyberbullying, online impersonation, hate speech, child pornography, etc. and caution the user that they are about to commit a crime and should self-regulate. Finally, emerging technologies can build human capacity to recognize online crimes and provide tools and resources to combat these, such as fact checker-, availability of consent, etc.

Original comments on the Miro board during the session:

- Capacity building for end-users to identify and prevent.
- AI is a powerful tool for detecting many forms of fraud, not just online.
- Supplement not substitute human moderators.
- Use AI to identify sexual imagery and build in a layer of consent for original image owner or don't allow posting.
- Good AI to fight bad AI, a never-ending race.
- Hate speech detection.
- Global Engine like Fact checker for fraud, online scams.
- Building awareness among end users even at grassroots levels - as simple as setting a strong password.
- Use tech to flag potential crimes for human review but do not allow machine adjudication.
- AI can train humans to identify disinformation.
- Pattern analysis and predict the potential for future activities of criminals.
- Adopt Open AI and share the technologies with developing countries.
- AI can identify trends in disinformation and help law enforcement.
- AI can have separate regulatory body.
- AI can be used to take down non-consensually shared images and info.
- Only using tech to address OGBV without humans has failed in the past.
- AI that's based on racist/casteist/queerphobic/ableist tech and biased data sets will be flawed. Cannot shy away from this. Need to course-correct urgently.

7.4 What is the role of the GDC in ensuring safeguards?

According to the participants, the GDC is critical for protecting online/offline privacy with AI and other disruptive technologies. Harmonizing regulations, guidelines, and standards for ethical AI use, establishing watchdog networks, and putting consumers first are key roles. Guidelines for responsible social media behavior, best practices for AI use, and assessing potential harm and benefits are needed.

Participants also agreed that safeguards must be in place at all levels, and AI's intended purpose and potential impact on individuals assessed before adoption. Balancing AI's use to detect bad behavior versus tracking people and driving consensus on common regulations is essential. Broad principles to govern AI, data usage by governments/corporations, evolving tech governance standards, and a sandbox for AI development are needed.

Safeguards against AI impacting jobs/livelihoods and a need for a regional/global regulator must be established. Furthermore, the participants suggested that national policies must promote safeguards for children's data privacy and safety. By implementing these measures, AI can be developed and deployed with more confidence and transparency.

Original comments on the Miro board during the session:

- Harmonization of the regulation, standards, and guidelines.
- Add networks of watchdog.
- Put consumer first.
- Guidelines for responsible behavior of social media platforms.
- Join mechanisms like global SOC to ensure safeguards.
- Gather best practices of AI use, its harm, and benefit.
- Issue an international treaty on cyber security for all UN member states to comply.
- Safeguards on the civil, political, economic, and personal levels.
- Clearly outline the intended purpose of AI systems and assess the overall potential impact, notably on individuals, before adoption.
- Principles to balance between using AI to detect bad behaviors vs using AI to track people.
- Drive consensus on common minimum regulations for AI use and application.
- Need a broader set of principles that govern AI.
- Guiding principles of usage of data by governments and corporations.
- Direct existing standards and tech governance bodies to evolve standards for emerging tech in a time-bound manner.
- GDC has convening power (to create good AI, sandbox environment).
- Principles of data sharing in government procurement contracts with third parties.
- People need to be part of decision-making in a democratic system / Need safeguards against AI impacting livelihoods and jobs.
- Develop broad standards and promote the need for a regulator either regional or global.
- Advocate for safeguards for children's data privacy and safety in national data privacy policies.

Additional aspects, added by a participant after the workshop:

Whilst it is impossible to predict the future, there seems a possibility that the current path of compounding exponential AI development could lead to an artificial superintelligence that for our practical purposes behaves as if it is self-motivated. Given the number of countries, companies, and individuals that could develop this with increasing ease, either intentionally or unintentionally, it is difficult to stop or regulate. A proactive precaution could be the creation of a mutual understanding between superintelligences and humanity that would set out principles of mutually beneficial coexistence and safeguards against negative outcomes. The drafting of such a document could be part of the GDC, which would be the ideal forum for such a consensus.

7.5 How can the GDC guide the development of a regulatory environment to build future ‘privacy by design’ technologies?

The participants discussed that the GDC can guide the development of a regulatory environment for privacy by design technologies by working closely with governments and providing them technical support to address violations, while also assuring a broader representation in the debates and standard-setting processes. Furthermore, the GDC could facilitate agreements on principles for AI and help introduce privacy by design as a requirement in public contracting sectors. It could also support requiring audits/transparency in donor-funded IT/AI systems. Participants agreed that the GDC should coordinate best practices, promote AI as a global good, and use AI for SDGs with transparency, explainability, accountability, and clear demarcation of no-go areas. It should also establish guiding principles for emerging technologies such as AI but should do so by adapting them to each sub-context.

Original comments on the Miro board during the session:

- Work closely with governments about privacy.
- Technical support for the government regarding the mechanism for GDC violation.
- Agree on a set of principles for AI for Good, and work with countries to adopt those.
- Privacy by design, followed by option for consent to collect data.
- Have greater representation in AI standard-setting bodies.
- Require privacy by design in public sector contracting and in public facing/influencing sectors.
- Procurement rules for all donor-funded IT/AI systems that governments build to have audits/transparency at deployment and throughout the life of system.
- Policy, best practice, and technology.
- Coordinate best practices.
- AI must be a global good.
- Using AI for SDGs.
- Transparency, explainability, accountability, and a clear demarcation of no-go areas.
- Emerging Technology
- Crucial to determine the sub principle-, the second layer of guiding principles for emerging tech: AI as a data amassing, black box tech that is labelled for exclusion will require a different kind of principles as compared to blockchain that adds immutability and transparency and have privacy related issues.
- GDC can monitor the AI - +.

8. Work Session (f): Bridging the capacity gap for developing countries in the emerging technologies domain

8.1 How can collaboration and sharing of technology and resources with developed countries look like?

To bridge the capacity gap in emerging technologies for developing countries, participants discussed the role of developed countries or technologically advanced countries in evangelizing impactful digital goods as public goods and setting up easy technology transfer mechanisms for others. Such digital goods with proven impact in one context could be tested across varying contexts to minimize new development costs. Participants also discussed using knowledge exchange between developing country decision-makers and policymakers to build collaborative solutions for similar country contexts thus maximizing the use of limited resources; focusing energies on building foundational or core technology infrastructure that allows for interoperability, sustainability, and sharing instead of investing in building siloed applications in the short term. Setting up a funding mechanism that developing countries can leverage to facilitate the aforementioned measures was also discussed.

Original comments on the Miro board during the session:

- The creating countries of highly impactful technologies have the onus of evangelizing this technology/resources with other countries and set up mechanisms for transfer (example: GOI + MoE + ekStep + DIKSHA platform).
- Provide scholarship on digital technology for representatives of marginalized groups from developing countries.
- Collaborative solutions to solve real and specific problems in the developing country, for eg. exchange between public officials.
- Preferably restrict public infrastructure to be between central agencies
→ need to be done with good intent, should not impact the data sovereignty of the developing country.
- Establish technology and resource repository and provide access to relevant stakeholders.
- Urge new technologies to be tested across a variety of contexts and this is facilitated by government collaboration agreements.
- Has to be needs-based.
- Focus on the core-technology and not just on applications.
- Best practices for making and enforcing related laws e.g. data protection laws.
- Sharing good practices among countries, including the details of the technology.
- Multilateral Fund.
- In case of DPGs - reputational risks need to be mitigated.

8.2 How should governments contribute to capacity building through funding, policies and infrastructure development?

Participants agreed that the role of governments of developing countries in capacity building for emerging technologies is to first reform and organize themselves to become agile and responsive to the evolving tech ecosystem by simplifying processes and policies. Second, governments should work with different stakeholders, such as industry associations and sector regulators, to invest in creating digital public infrastructure, digital frameworks, and architecture which serve as the backbone for all other applications development efforts, and to build local, and national capacities in the long term. And finally, the governments should convene with the private sector and academia to raise capital for investments in infrastructure development and R&D in emerging technologies.

Original comments on the Miro board during the session:

- Convening private sector, and communities (venture capital?).
- Overcome institutional inertia.
- Political will & capital are key.
- Engage industry bodies and sectoral regulators to drive funding policies and spur development.
- Establish Government Funding in Capacity Building and R&D and create ecosystem between industry, academia, and government.
- Open Source all research funded by public money and make this available to global research networks.
- Govt. led sectoral development of policies and public infrastructure, where all stakeholders come together.

8.3 How can local innovation and entrepreneurship be incentivized?

To build capacity through local innovation and entrepreneurship, different stakeholders such as government, private sector, academia, industry associations, and young people, need to come together for fostering an ecosystem that allows for experimentation and healthy competition; provides access to funds, resources, and mentoring; simplifies start-up registration processes and provides tax incentives; and establishes a culture of innovation in schools and communities.

Original comments on the Miro board during the session:

- Provide public/grant funding not only for DPGs for DPI, but DPGs that have a criteria to prototype on a self-sustainable model. This prototype funding will help unlock traction to show for private investors - which needs to be pooled together.
- Let local innovation/entrepreneurship foster without too many DOs and Do NOTs.
- Provide funding and resources.
- Without recognizing some parts of digital system as DPIs, and as a commons, local innovation and entrepreneurship are not possible.
- Easy access to mentorship.
- AI reduces startup costs, which provides opportunities for emerging countries and disadvantaged groups.
- Governments and the UN can encourage and convene startup competitions on social impact.
- Data spaces and data pools should be commons, this will allow local innovation and businesses. EU's digital strategy has data spaces as its central items.
- Provide network for entrepreneurs and how this network is open to supporting them.
- Innovation for the sake of mere innovation will not work.
- A culture of innovation needs to be embedded in the education systems. Cannot be incentivised suddenly.
- No complicated registration for new startups; provide opportunity in local projects; Tax incentives.

8.4 Which partnerships are required with the private sector and research organizations?

The private sector should engage more closely with academia, and young people should participate in creating and owning digital public goods. Private sector engagement in the development sector

should go beyond mere CSR, and champions should be identified in innovation hubs within countries that have the necessary network and values for creating DPGs.

Original comments on the Miro board during the session:

- Private sectors should closely engage with academia - young people on campuses should participate in creation and ownership of DPGs.
- Presently a lot of private sector engagement in development sector is through CSR. Can it move beyond mere ticking of checkboxes?
- Identify champions in the innovation hubs within countries who have the network and values in relation to the creation of DPGs.

8.5 Which mechanisms are necessary to access international knowledge-sharing and collaboration?

To access international knowledge-sharing and collaboration, there needs to be digital literacy for all. Participants stated that funding, computing, and resources are concentrated in the private sector, so academia must be strengthened to research alternate tech models.

Original comments on the Miro board during the session:

- Collaboration comes at a cost.
- Risk of Chinese standard setting campaign.
- Funding, compute, resources concentrated in the private sector. Academia must be strengthened to research alternate tech models.
- Digital literacy for all, globally.
- Global knowledge/ resource sharing.

8.6 What is the role of academia and industry to address the capacity gap?

The role of academia also extends to building digital literacy skills for everyone, encouraging young people on campuses to participate in the creation and ownership of DPGs, providing students access to global scholarships and funds for training in emerging technologies, introducing a curriculum that spurs innovation and entrepreneurship and allows inter-disciplinary approaches to innovation. It is also desirable that private sector partners should have intentional, long-term engagement objectives beyond minimum CSR requirements.

Original comments on the Miro board during the session:

- Academia has the ability to reach young people and also young people who have the ability to build technology for good and designed with principles in mind.
- Researching about the trends, good practice to reduce the capacity gap.
- Incentivize (e.g. tenure points) policy relevant output production from research.
- Build curricular on tech ethics. Incorporate into any IT/CompSci degree.
- Researching on new technology by the Academia is an important factor that needs to be considered.
- Incentivize academia through funding to see where tech can break and solve for that before it hits mainstream.
- Interdisciplinary courses eg law and tech.
- Integrate Design Principles for Development.
- Awareness of open-source self-sustainable business models.
- Intentional efforts need to be done to support and incentivize women, BIPOC, people from oppressed castes, and LGBTQ participation.

- Loss of diversity = Loss of innovation/money/knowledge.

8.7 How can capacity-building be implemented to strengthen developing countries' position on emerging technologies?

Participants agreed that global scholarships and funds can be provided to enable students and researchers to study these technologies abroad and establish research centers back in their home countries. The G20 process can also be used, and participation in official internet governance processes is important. Additionally, capacity building is necessary for local experts to adopt emerging technologies provided and shared by developed countries.

Original comments on the Miro board during the session:

- Use G20 process.
- Global scholarships and funds that enable students and researchers from developing countries to study these technologies abroad and establish research centres back in their home countries.
- Developing Countries are lack behind of skill human resources in emerging technologies. Capacity Building is necessary to local experts to adopt the emerging technologies provided and shared by a developed country.
- Participation in official internet governance making processes.

8.8 How can the GDC recommend sustained capacity development measures that are attainable?

To support entrepreneurs, resources should be pooled together, such as network platforms and funds. Provision of technology and training should also be provided. However, the challenge of knowledge gatekeeping needs to be addressed as knowledge is often locked behind paywalls. Knowledge commons on technology can be created, and gatekeeping mechanisms can be removed while balancing copyright/copyleft, which should be done by a global body.

Original comments on the Miro board during the session:

- Pool together resources for entrepreneurs for immediate benefits available - network platform, fund.
- Provisions to provide technology + person to teach it.
- How to address and challenge gatekeeping of knowledge? - knowledge is locked up (by gatekeepers/behind paywalls) and we are funding existing knowledge mechanisms only.
- Knowledge commons on technology.
- Remove gatekeeping mechanism while balancing copyright/copyleft (this has to be done by a global body).

9. Work Session (g): Security by Design: Technologies that can be scalable and affordable

9.1 What are the risks associated with open and accessible technology?

This session is covered by answers to three questions. The first question is about the risk associated with open and accessible technology. Participants discussed continuity, availability, and affordability for all the stakeholders is a question and GDC needs to be seriously considered on this matter. Another main risk highlighted is that open and accessible technologies can be misused, abused, and customized for illegal purposes and there should be a consideration on this issue.

Furthermore, it is discussed how open technology needs to be sustained with continuous contributions from those who have the capacity to adopt it in the local context. Another main problem discussed was security. Privacy and ethical guidelines are well developed but, unfortunately, developers are not seriously concerned about those and there is a need to address these matters at the global level.

Original comments on the Miro board during the session:

- Continuity
- Availability for all the stakeholders is a question.
- Need resources to track changes and improvements.
- Not moving to maturity.
- Guideline on open and accessible technology.
- Identity theft, privacy, and security of individual data.
- It is imperative that any open and accessible technology should not take away the agency from the private organizations need for innovation and capacity building.
- Difficult to scale for larger organizations, esp government.
- Depends on how you define open - open source is not insecure.
- The risk associated with open and accessible tech lies in the interpretation of the vocabulary here: what is meant by open and accessible; a narrowly framed understanding runs the risk of giving the illusion of being fair.
- Responsible Tech.
- Trade-offs - making tradeoffs expensive through liability.
- Open and accessible technologies can be misused, abused, customized for other purposes.
- Understanding the vicious circle -insurance, anti-virus and other derivative businesses a security glitches.
- Open technology needs to be sustained with continuous contributions from those who have the capacity to adopt them locally
- No guidelines for security, privacy, and ethics are followed by the developers.
- Don't continue developing and eventually become stale and unusable.
- Fail to build capacity of the adopters and community.
- Open tech not becoming open as a result of "National Security" claims of bad actors.

9.2 What are the present concerns on cyber security and the safety of digital technologies?

The second question relates to current concerns about cyber security and the safety of digital technologies. The participants were discussing the lack of common understanding of what's safe and unsafe is a common issue faced and it is a consideration that needs to be addressed by the respective authorities. Another main problem discussed in this forum is fake news spreading, which is harmful to national and international political levels. Online fraud and related laws protected to

victims need to be protected by the judicial system and in addition to that cyberbullying and identity theft also need to be considered. Furthermore, it is highlighted that the lack of awareness at the developer level about security and safety standards needs to be considered. Additionally, participants highlighted that the lack of awareness at developer level about contextual security and safety standards also needs to be considered. One other group member highlighted a conceptualization and operationalization of cybersecurity that is centered on people and their rights and experiences.

Original comments on the Miro board during the session:

- Identity theft.
- Lack of security and privacy incorporation.
- Dark web.
- Lack of common understanding of what's safe/unsafe.
- Fake news, online fraud, cyberbullying, identity theft, etc.
- Usually less user-friendly and time-consuming because there are more security layers.
- Using online infrastructure and services without proper knowledge.
- No regulatory governs cross border tech company.
- Fraud and cyber thefts/crimes.
- Lack of awareness at the developer level about security and safety standards.
- No framework of standards available for developers to follow or adhere to.
- A conceptualization and operationalization of cybersecurity that is centered on people and their rights and experiences.
- Platforms operate in a liminal space as far as law is concerned.
- Contextual security and safety standards are needed.

9.3 How can the GDC recommend 'basic security and safety' measures that could be incorporated into designing technologies?

The next problem discussed was how GDC could recommend basic security and safety measures that could be incorporated into designing technologies. Participants mainly highlighted having high-level guidelines and when developing such guidelines, collaboration with a network of communities around cyber technology needs to be considered. Furthermore, it is mentioned that the requirement of governance for technologies, especially ones that are applied for public purposes. In relation to the human rights concern, concerns highlighted, that principles for security and safety need to be considered. Furthermore, in the future, it is necessary to have more concern about Artificial Intelligence security. The need to mandate data protection and hold regular audits are proposed as best practices.

Original comments on the Miro board during the session:

- Develop some high-level guidelines.
- The private sector would be receptive to regulation, as commercial pressure from investors, clients and competitors make them release AI faster than they would like.
- It should not get into specific technology measures or fixes.
- Collaborative with network of communities around cyber tech.
- Need to move to more memory safe language.
- Require governance of technologies especially ones that are applied for public purposes.
- Principle for security and safety with respect to human right.
- Need to educate customer on the security front.
- Focus on AI security.

- Need to mandate data protection and hold regular audits. Some best practices such as end-to-end encryption should be done. Need to incentivize as well as punish.
- Cannot have a one size fits all model of security.
- Principles of openness need to be carried with security.

10. Work Session (h): Capacity Building for developing countries in cyber security

10.1 What are the mechanisms to strengthen human resources in cyber security at scale and affordable cost?

The last session will discuss two main questions, first, what mechanisms are in place to strengthen human resources in cyber security at an appropriate scale and at an affordable cost. Many participants were discussing having developed internationally recognized training courses which should not cost and proposed to deliver them through volunteer experts. In relation to awareness of cyber security, there is not only a specific group of people, but also different levels of people, including those covering different job categories, and different levels of people who have adapted technology to different adaptation levels. It is proposed that everyone should be familiar with fundamental cyber security aspects, and it is proposed to include this in the school curriculum as a part of the skill development of digital literacy for the smaller and younger generation to create awareness of cyber security. Further, it is mentioned that having stakeholders at all levels including governments, frontline workers, legal and accounting professionals, the media, etc is needed to consider this process. Additionally, it is mentioned that developing guidelines for a dedicated cyber security university degree is important and another participant mentioned that to have already included a cyber security degree program in the IEEE Guidelines for developing university degree programs as a benchmark. One proposed idea is to include cyber security as a compulsory module under co-subject in all the other computing degrees such as computer science, computer engineering, Software engineering, Data Science, Information Technology, and Information Systems. Furthermore, establishing fellowships to train and build capacity was suggested under this question.

Original comments on the Miro board during the session:

- Develop internationally recognised training courses and deliver them through volunteer experts.
- Awareness of all the level.
- Everyone should be familiar with fundamental cyber security aspects.
- Provide free and open resource on cybersecurity.
- Cyber security should be part of Digital literacy skills in schools.
- Understand the needs of stakeholder at all levels - from govt, technical person, general consumers.
- Develop guideline for dedicated cyber security degree in University.
- Human resources should be thought of widely - govt, frontline workers, legal and accounting professionals, media, etc.
- Establish fellowships to train and build capacity.
- Create jobs in govts and companies to stimulate the demand.

10.2 How can universal implementation of cyber security among all countries be achieved?

The second question focuses on how universal implementation of cyber security among all countries can be achieved. It was discussed among group members and the first suggestion was to have an agreement or treaties to prevent cyber-attacks from one country on another and examples were given, like the US on Brazil, and China on the African Union. Furthermore, participants discussed creating or scaling up Public Service Announcement (PSA) campaigns for cyber security.

Another - contested - idea, said that it will be very difficult due to resource diversification in the universal implementation of cyber security among all countries. And also, it is indicated that defining common minimum standards is important and it is necessary to implement them with the specifics of the different sectors in mind. Participants also discussed about the three levels (including government, company, and personal level) which can be addressed by regulation in a combined way. Furthermore, it was discussed to implement CSR for cybersecurity.

Original comments on the Miro board during the session:

- Agreements or treaties to prevent cyber attacks from one country on another (like US on Brazil, China on African union etc).
- Create/scale up PSA campaigns for cyber security.
- It will be very difficult due to resource diversities.
- Cyber security standards developed specifically to sectors.
- Define common minimum standards.
- Would a universal cybersecurity implementation protect journalists and activists from mega surveillance systems like Pegasus?
- Urge CSR for cybersecurity.
- Treaties or Conventions on Cyber Security.
- Solution: using standards and guidelines. V/S Standards will be based on basis of necessities.
- There are three levels - government, company, and personal - which can be combined by regulation.
- Shared Awareness Contents that can be localized.
- Need to identify common grounds using universal discussions and mediated processes.

11. Closing Remarks

11.1 Muanpuii Saiawi, Joint Secretary, Cyber Diplomacy, Ministry of External Affairs India

The Joint Secretary for Cyber Diplomacy is expressing her gratitude for the successful conclusion of the United Nations Global Digital Compact multi-stakeholder regional consultations in New Delhi, co-hosted by India and Germany. She thanks the participants for their diverse perspectives, experiences and expertise, which have shaped the direction and content of the Global Digital Compact and highlights the importance of this once-in-a-lifetime-opportunity to shape the digital future for all.

The Joint Secretary further goes on to ensure that the GDC reflects the rich diversity of perspectives and the complexities of the digital landscape and, moving forward, she recognizes that digital transformation is ongoing and rapidly evolving, and therefore we must continue to work collaboratively and inclusively.

Ms. Saiawi highlights the potential of the GDC to address the aspirations of developing countries in Asia and emphasizes the need for ongoing collaborative and inclusive work to ensure that the benefits of digital transformation are harnessed for developing countries' growth and socio-economic development. Lastly, she acknowledges and thanks the co-hosts, facilitators, moderators, and participants for their contributions to the event.

11.2 Ambassador Anna Karin Eneström, Permanent Representative of Sweden to the UN

Ambassador Eneström firstly thanks all participants and states that she has been impressed by the comprehensive, high-level creative ideas and views expressed during the Asia Consultation from so many different stakeholders. She points out that she has taken notes and will bring what has been said with her back as she continues the process of elaborating on this common vision of a Global Digital Compact. And what she has heard during these full and fruitful days will be brought into the continued process.

Lastly, she acknowledges and thanks the co-hosts, facilitators, moderators, and participants for their contributions to the event.

11.3 Regine Grienberger, Cyber Ambassador, Federal Foreign Office Germany

The German Cyber Ambassador expresses her gratitude to the participants for their valuable contributions during consultations on digital issues and the positive impressions gathered through these regional consultations. She mentions that she will share notes with her team and points out that there are many commonalities in digital regulation discussions across regions, including Europe, on regulations, Digital Public Goods, public infrastructure as well as cyber security.

Dr. Grienberger states that the EU has finalized its contribution to the Global Digital Compact, which emphasizes a commitment to a multi-stakeholder process, digital rights, and global governance for the digital age.

12. Conclusion and perspectives towards the future

The GDC Asia consultations held in New Delhi, India, marked the end of the other regional consultations that also took place in Mexico in February 2023 and in Kenya in December 2022.

The inputs from these consultations, the submissions to the UNSG's Envoy on Technology through the provided online tools and policy briefs will inform the GDC that will be agreed on at the Summit of the Future in September 2024, whose theme, 'multilateral solutions for a better tomorrow' appropriately reflects the intent of the GDC in the fast-evolving digital arena.

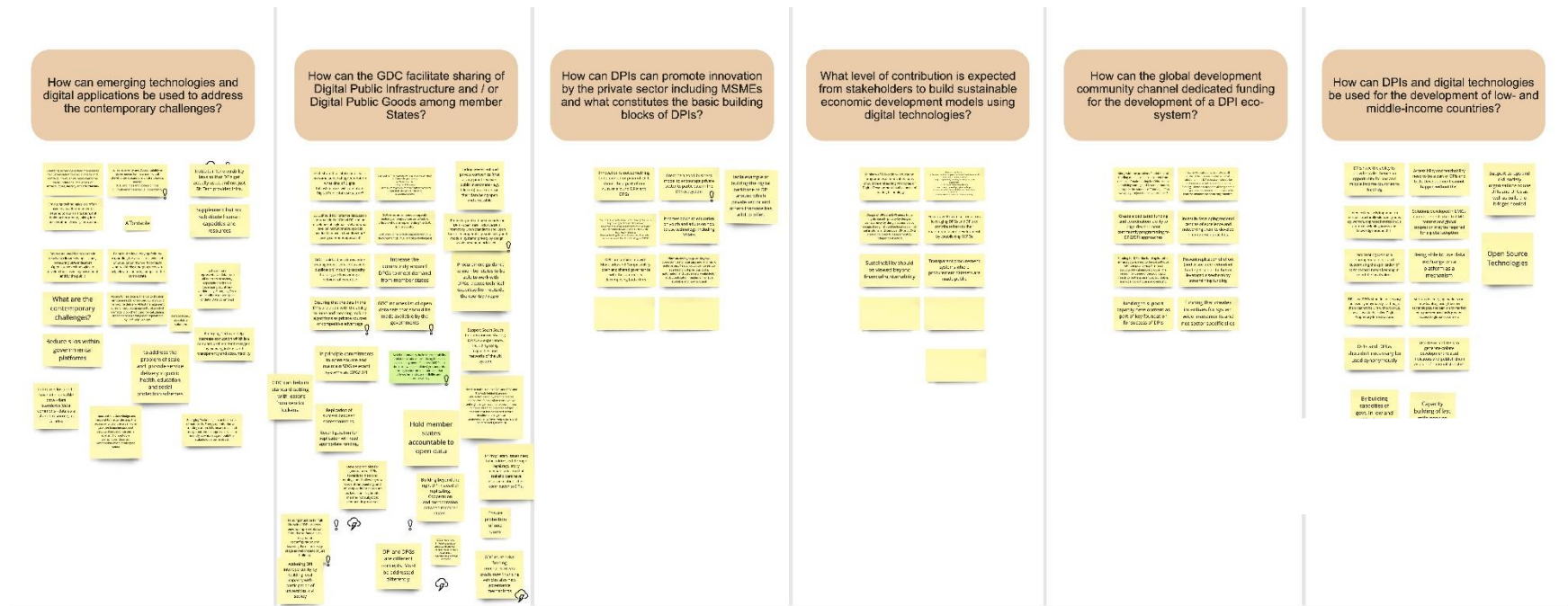
There has been diverse participation - especially the participation of so many inspiring women expert digital leaders - in the Global Digital Compact Asia Regional Consultation. The sessions were organized in a multi-stakeholder format with deep dives to facilitate in-depth discussions in smaller groups, to then come up with recommendations for the GDC. The discussions and conversations have focused on digital inclusion, addressing the digital divide, capacity building - especially for the global south - as well as on cyber security and other aspects of trust and security online and the data dimension of the digital world. The discussion on Artificial Intelligence and other new emerging technologies has been particularly interesting. The present report will be a valuable contribution to the Global Digital Compact.

The presence of the co-facilitators of the process for the GDC - the Representatives of Sweden, the Ambassador to the UN, and Rwanda - was of particular importance as they were able to listen in to the discussions and bring key aspects of the Asia Regional Consultations into the process overall. In the following month, based on the inputs received as well as other consultations and research conducted by the United Nations, the Office of the Envoy on Technology will compile the material and present this to United Nations Member States, preparing for the deliberations for the GDC during the 2024 'Summit of the Future'.

Annex.

Role of Digital Public Goods (DPG) including Digital Public Infrastructure (DPI) in the GDC to achieve the 2030 Agenda

Work Session (a)



🗨️ = disagreement among participants
 ⚡ = resonates strongly among participants

Key messages towards the GDC:

- 1. Digital Public Goods (DPGs) are essential for achieving the Sustainable Development Goals (SDGs) and the 2030 Agenda.
- 2. Digital Public Infrastructure (DPI) is a key enabler for DPGs and economic growth.
- 3. Collaboration and partnerships are crucial for the development and sharing of DPGs and DPI.
- 4. Funding mechanisms need to be developed to support the development of DPGs and DPI.
- 5. Digital literacy and skills development are important for the effective use of DPGs and DPI.
- 6. Digital Public Goods (DPGs) can be used to address contemporary challenges such as climate change, inequality, and digital divide.

Inclusion and gender equality in global digital transformation

Work Session (d)

How can we ensure inclusive participation?

Ensures user participation across a variety of users and gender identity with a rich diversity, race, ethnicity.

- Gender is not just man or woman.
- Inclusive participation in policy spaces, meetings, groups, etc. with meaningful representation
- Let's Think beyond binaries in gender
- Ensure that all digital platform accessible for all
- Consultation with representatives of diverse groups should be done from the design to the evaluation
- Ensure meaningful participation of the most marginalized and intersectional vulnerable groups
- Beneficiaries should be included in the consultation and be central in the decision making process.
- Multi stakeholders process involvement in digital development
- It is necessary to identify parents but not to place a particular focus on what a parent is doing, but rather on what a parent is not doing, such as digital literacy or skills, wage negotiations, but also on what a parent is doing.
- Gender should not be a "niche" topic
- Recognize that solution is not for everyone. It may be for some groups and not for others.
- Cross media mechanisms in partnership with organizations that have an established reputation for trust to create holistic, open and programmatic solutions
- Diverse hiring practices in tech companies and diverse student recruiting practices in university and non-academic settings
- Have multiple gender representations while designing - "Inclusion by design?"
- Participatory design

How can we bridge the digital gender divide?

An intersectional gender approach to access and the application of human rights criteria, with specific attention to online gender-based violence and gendered digital divide.

- More girls in Tech - STEM right from the beginning
- Building analog foundations first
- addresses issues of gender and social institutional discrimination
- work bottom-up - identify community champions
- Cover diversity groups
- Use tech to combat crimes
- Gender Obsolescence
- Work on changing "gatekeeping" mindset towards women
- Contextual engagement: Barriers rules can do more harm than good
- Gender sensitive data collection and gender disaggregated data publication (data related to digital)
- Short term solution - Focus on men and/or perpetrators of violence. Change THEIR hearts and minds
- Short term solution - Women sales agents at phone hops
- Address education from the school years, social awareness and skills development from school to participate in the digital world

How can we increase/ensure digital literacy, awareness and skills?

- CSW67 Conclusions have good language on this (needs to be more gender diverse inclusive)
- Digital literacy online needs to include access to sexuality, SHHR, abortion, gender identity education.
- Need to address the unpaid labour done by women in tech skills that are present are unacknowledged/uncredited
- First, connectivity to the internet must be addressed
- Ensure affordable digital devices
- Conductivity for CSO, so that they can digital skills for end users, the most marginalized groups
- address digital literacy divides
- Allocate the state budget for sufficient digital facility for marginalized groups
- Provide online specific services, not overly dependent on apps that what needs are accessible on such a wider internet connectivity
- Account raising for the governments about the importance of a digital accessibility for the most marginalized groups
- Private sector has a part to play when it comes to inclusion and upskilling their workers on digital literacy
- Mandate minimum digital literacy training for all working groups
- Let's avoid preaching whilst communicating
- make it part of school curriculum within K-8 grades

Key messages towards the GDC:

- Disagreement among participants
- Resonates strongly among participants

Impact of Artificial intelligence, machine learning, and emerging Technologies on online/offline privacy and protection

Work Session (e)

What are the risks associated with the AI, ML and other disruptive technologies to online/offline privacy?

- Risk of inaccessibility**: Reduced to lower levels of digital literacy, digital skills, and digital access.
- Accessibility in the after thought**: People in learning countries are left behind.
- Outdated hardware, especially for the poor**: Applications, browsers, or ML systems in the risk of progressing those already marginalised.
- Also needs AI to be fair by design**: Future of jobs: 60 percent of jobs are being automated without human input. What skills do young people need and how can we ensure we provide them through formal education and other pathways?
- Privacy by design**: Risk of government surveillance, data breaches, and other risks.
- no transparency on the backend coding system of AI**: Govt actors are centralised, but actors are decentralised.
- AI is a paradigm, not just a tool**: Many AI and ML, with other emerging tech, like blockchain, may be required for its potential to embed, cut and re-configure and accountability in the ecosystem.
- AI cannot be a silver bullet**: Many AI and ML, with other emerging tech, like blockchain, may be required for its potential to embed, cut and re-configure and accountability in the ecosystem.
- Privacy is a very narrow framing**: The term of AI is much broader and far reaching.
- Train AI with public data, but AI model is not public good**: Train AI with public data, but AI model is not public good.

How can AI, ML be used to identify and fight against misinformation and disinformation which may be generated by AI, ML?

- Include responsible use licenses for generative AI**: No one should own the data they use to represent themselves with generative AI.
- Global trusts: AI and ML Engine to detect, transform and disseminate**: Global trusts: AI and ML Engine to detect, transform and disseminate.
- good AI to fight bad AI, a never ending race**: By using machine and deep learning, we can detect and identify disinformation and disinformation.
- AI literacy - train more people to access it**: AI literacy - train more people to access it.
- Privacy by design**: Risk of government surveillance, data breaches, and other risks.
- AI is a paradigm, not just a tool**: Many AI and ML, with other emerging tech, like blockchain, may be required for its potential to embed, cut and re-configure and accountability in the ecosystem.
- AI cannot be a silver bullet**: Many AI and ML, with other emerging tech, like blockchain, may be required for its potential to embed, cut and re-configure and accountability in the ecosystem.

How can emerging technologies be used to protect against online crimes?

- Goodly building for end-users to identify and prevent**: Goodly building for end-users to identify and prevent.
- AI is a powerful tool for detecting every form of fraud, not just online**: AI is a powerful tool for detecting every form of fraud, not just online.
- Supplement not substitute human moderators**: Supplement not substitute human moderators.
- good AI to fight bad AI, a never ending race**: By using machine and deep learning, we can detect and identify disinformation and disinformation.
- Hate speech detection**: Hate speech detection.
- AI can train human to identify disinformation**: AI can train human to identify disinformation.
- AI can identify trends and help user behaviour**: AI can identify trends and help user behaviour.
- AI can be used to take down non-consensually shared images and info**: AI can be used to take down non-consensually shared images and info.
- AI**: AI.
- Only using tech to address OGBW without humans has failed in the past**: Only using tech to address OGBW without humans has failed in the past.
- AI must be based on individualised case-by-case basis and biased data sets will be flawed. Content only using these data, lead to course correct regularly**: AI must be based on individualised case-by-case basis and biased data sets will be flawed. Content only using these data, lead to course correct regularly.

What is the role of the GDC for ensuring safeguards?

- Harmonisation of the regulatory standards and guidelines**: Harmonisation of the regulatory standards and guidelines.
- add networks of watchdog**: add networks of watchdog.
- put consumer first**: put consumer first.
- Guidelines for responsible behaviour of social media platforms**: Guidelines for responsible behaviour of social media platforms.
- Joint mechanism like global SDG to ensure safeguards**: Joint mechanism like global SDG to ensure safeguards.
- gather best practice of AI use, its harms and benefits**: gather best practice of AI use, its harms and benefits.
- Issue an international treaty on AI**: Issue an international treaty on AI.
- Safeguards on the civil, political, economic, and personal levels**: Safeguards on the civil, political, economic, and personal levels.
- Need a broader set of principles which govern AI**: Need a broader set of principles which govern AI.
- Guiding principles of usage of data by governments and organisations**: Guiding principles of usage of data by governments and organisations.
- GDC has convening power to create good AI samples, endorsement**: GDC has convening power to create good AI samples, endorsement.
- Need safeguards against AI impacting livelihoods and jobs**: Need safeguards against AI impacting livelihoods and jobs.
- People need to be party to decision making in a democratic system**: People need to be party to decision making in a democratic system.

How can the GDC guide the development of a regulatory environment to build future 'privacy by design' technologies?

- Work closely with governments about privacy**: Work closely with governments about privacy.
- technical support for the government, if the institution for GDC violation**: technical support for the government, if the institution for GDC violation.
- Agree on set of principles for AI for GDC, one with with countries to account for**: Agree on set of principles for AI for GDC, one with with countries to account for.
- Privacy by design, followed by codes for content in online data**: Privacy by design, followed by codes for content in online data.
- have greater representation in AI related setting bodies**: have greater representation in AI related setting bodies.
- Issue a global treaty on AI**: Issue a global treaty on AI.
- Policy, best practice and technology**: Policy, best practice and technology.
- Coordinate best practices**: Coordinate best practices.
- AI must be a global good**: AI must be a global good.
- Using AI for SDGs**: Using AI for SDGs.
- transparency, explainability, accountability, and a clear demarcation of no-go areas**: transparency, explainability, accountability, and a clear demarcation of no-go areas.
- Emerging Technology**: Emerging Technology.
- GDC can monitor the AI**: GDC can monitor the AI.

Key messages towards the GDC:

- AI, ML, need to be based on high data and no, big data for diagnosis and analysis. AI for prediction models, not drawing clear causal correlations.
- This will build towards greater accountability and responsibility.

52

Bridging the capacity gap for developing countries in emerging Technologies domain

Work Session (f)

How can collaboration and sharing of technology and resources with developed countries look like?

Has to be Needs based

Multilateral Fund

In case of DIPDS - reputational risks need to be mitigated

How should governments contribute to capacity building through funding, policies and infrastructure development?

Converting private sector, common files (venture capital)

Overcome institutional inertia

Political will & capital are key

How can local innovation and entrepreneurship be incentivized?

Provide funding and resources

Build

Easy access to mentorship

Which partnerships are required with the private sector and research organizations?

Which mechanisms are necessary to access international knowledge-sharing and collaboration?

Collaboration comes at a cost

Digital literacy for all, globally

What is the role of academia and industry to address the capacity gap?

Interdisciplinary courses eg law and tech

Intergrate Design Principles for Development

How can capacity-building be implemented to strengthen countries' position on emerging technologies?

Use G20 process

How can the GDC recommend sustained capacity development measures that are attainable?

Knowledge commons on technology

Key messages towards the GDC:

Security by Design: Technologies that can be scalable and affordable

Work Session (g)

What are the risks associated with an open and accessible technology?

continuity	Availability for all the stakeholders is a question	need resources to crack changes and improvements
not moving to maturity	guideline on open and accessible technology	identity theft, privacy and security of individual data.
Responsible Tech	Difficult to scale for larger organisations esp government	branches or how you define open tech source is not secure
Open tech not becoming open as a result of "National Security" claims of bad actors	understanding the vectors of the intelligence and what is done in the future businesses a security pillars	Open tech requires to understand the vectors of the intelligence and what is done in the future businesses a security pillars
	Don't continue moving up and eventually become stale and unuseful.	Fail to build capacity of the adopters and community.

Open tech not becoming open as a result of "National Security" claims of bad actors

What are the present concerns on cyber security and safety of the digital technologies?

Identity theft	Lack of security and privacy incorporation	dark web
lack of common understanding on what's safe / unsafe	Risks, more, online fraud, opportunity to identity theft, etc	Identity loss, job friendly and time consuming because more security steps
Lack of awareness at developer level about security and safety standards	No regulatory agencies across sector tech company	Fraud and cyber thefts/crimes
Platform to operate in a digital space as far as law is concerned	No framework of standards are able for adopters to follow or others to	A conceptualisation and operationalisation of cybersecurity that is centred on people and their rights and experiences.

How can the GDC recommend 'basic security and safety' measures that could be incorporated into designing technologies?

Develop some high level guidelines	Need to move to more memory safe language	Focus on AI security
collaboration with network L3 communities around cyber risks	Need to Educate customer on the security front	principles of openness need to be carried with security
principle for security and safety with respect to human eye	Cannot have a one size fits all model of security	

= disagreement among participants
 = resonates strongly among participants

Key messages towards the GDC:



Capacity building for developing countries in cyber security

Work Session (h)

What are the mechanisms to strengthen human resources in cyber security at scale and affordable cost?

ensure that all employees receive training on the latest developments in the security aspects	Awareness of the all the level	everyone should be familiar with fundamental cyber security aspects
provide free and open resource on cybersecurity		cyber security should be part of digital literacy skills in schools
understand the needs stakeholders at all levels: brand, product, service, general consumers	Develop guidelines for digital cyber security literacy for the industry	human resources should be trained to include cyber security in their work, especially when they are involved in work, etc.
establish fellowships to train and build capacity	increase in grants and incentives to stimulate the demand	

How can universal implementation of cyber security among all countries be achieved?

it will be very difficult due to resource diversities	Create/scale up PSA campaigns for cyber security	agreement on baseline to prevent cyber attacks from spreading and protect the critical infrastructure in the region
Cyber security standards developed specific in sectors	define common minimum standards	What is the role of standards in the regional context? How to ensure that standards are adopted and implemented in the region?
Urge CSR for cybersecurity	Treaties or Conventions on Cyber Security	Need to align the demand for standards with the needs of the region
There are few levels: government, industry and academia, and it is difficult to coordinate by themselves	Shared Awareness contents which can be localized	Need to identify common grounds using national or regional level initiatives

= disagreement among participants
 = resonates strongly among participants

Key messages towards the GDC:

