वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

DIGITAL ECONOMY MINISTERS MEETING

Outcome Document & Chair's Summary

Bengaluru, Karnataka

August 19, 2023

G20 Digital Economy Ministers Meeting
Bengaluru, August 19, 2023

Outcome Document and Chair's Summary

The Outcome Document comprises the entire text, which was unanimously agreed to by all G20 members, except for Paragraph 24 which pertains to the Chair's Summary

Introduction

1. We, the G20 Ministers responsible for the digital economy, met on 19 August 2023, at Bengaluru to deepen our discussions on digital innovation and inclusion, digital skilling, and security in the digital economy.

2. We recognise the importance of creating an enabling, inclusive, open, fair, non-discriminatory, and secure digital economy. In the context of digital economy, we also respect applicable legal frameworks. We take cognizance of the critical role played by digital technologies in helping the world navigate the myriad challenges posed by the COVID-19 pandemic and the lack of technological and financial capacity in many countries to develop and deploy well-designed, inclusive, secure, trusted, resilient, sustainable, open, safe, and interoperable digital systems that respect human rights to unleash the potential of the digital economy. Therefore, we acknowledge the importance of adopting an inclusive, sustainable, development-oriented and human-centric approach that protects privacy and data, to respond to various challenges and leverage opportunities of digitalisation.

3. We acknowledge that digital divides, including the gender digital divide, are a considerable challenge for all countries, especially in developing and least developed countries. Noting our deliberations to bridge the digital divides undertaken during previous G20 presidencies, we reaffirm the urgency to accelerate inclusive digital transformation for all, especially for underserved groups and people in vulnerable situations.

4. We recognise that the availability and accessibility of high-quality digital connectivity based on sustainable, high-performance, secure and resilient digital infrastructure is critical for the future. Building on G20 achievements over the years, we reaffirm our commitment to bridge connectivity gaps, and encourage the goal of promoting universal and affordable access to connectivity for all. While we continue to welcome global efforts towards universal connectivity, we seek to collectively work towards making connectivity more meaningful, by empowering users and maximising the benefits of the Internet for all in order to facilitate economic growth and sustainable development.

5. We recognise that accessible, inclusive, secure, and safe digital systems have the potential to drive the economy of the future and catalyse growth, innovation, education, and sustainable development. We also reaffirm the importance of

security in the digital economy as a key enabling factor and recognise that digital skilling initiatives can accelerate the growth of the digital economy.

A. Digital Public Infrastructure for Digital Inclusion and Innovation:

6. Under the Indian Presidency's initiative, we recognise that digital public infrastructure, hereinafter referred to as DPI, is described as a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and / or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms. Considering the diverse approaches of G20 members to digital transformation, we recognize that DPI is an evolving concept that may not be limited to sets of digital systems with these characteristics and could be tailored to specific country contexts and can be referred to with different terminologies.

7. Meaningful connectivity can be enhanced through human-centric, development-oriented, sustainable, scalable, secure, accessible, and inclusive digital systems, such as DPI, that have demonstrated their potential. As technological advancements continue to offer opportunities to transform public and private sector service delivery, DPI offers a promising approach to digital transformation by providing a shared technology infrastructure that can be built and leveraged by both the public and private sectors. During the COVID-19 pandemic, DPI demonstrated its effectiveness by enabling easier access and delivery of services through innovative public and private sector solutions. When developing, deploying, and governing DPI we note the importance of prioritising secure and inclusive approaches that respect human rights and protect personal data, privacy, and intellectual property rights. For this, we recognise the importance of governance frameworks and institutional capabilities that seek to ensure that DPI is safe, secure, trusted, accountable, and inclusive. We also recognise the role DPI can play in furthering meaningful connectivity and accelerating progress toward implementing the 2030 Agenda for Sustainable Development and achieving Sustainable Development Goals (SDGs).

8. We underline the importance of sharing domestic experiences and learnings in the development and deployment of DPI, within and beyond the G20, to fully harness the opportunities offered by DPI and provide reference to other countries, including Low-and-Middle-Income Countries (LMICs). Towards this, we welcome the **G20 *Framework for Systems of Digital Public Infrastructure*** (**Annexure 1**), a voluntary and suggested framework for the development, deployment, and governance of DPI. The framework covers the technology as well as non-technology components, which include governance and community, along with the suggested principles for building robust, inclusive, human-centric, and sustainable DPI. We also note that the framework provides flexibility to G20 members and other countries in terms of choice of technology and approaches to DPI. We affirm the importance of ensuring appropriate levels of privacy and data

protection in accordance with applicable legal frameworks. We take cognisance of some of the basic DPI for domestic purposes, such as digital identity, digital payment systems, and data-sharing mechanisms with consent wherever applicable, among others, which can enable secure identification, fast and reliable payments, and seamless exchange of data/information respectively. They can also act as foundational layers across sectors like health, agriculture, manufacturing, and education among others.

9. Within the context of DPI, we recognise the importance of promoting open-source software, open Application Programming Interfaces (API) and the standards that support them, including open standards, to enable different DPI systems to communicate, with cross-border interoperability as a long-term goal. We reaffirm the importance of enabling cross-border data flows and data free flow with trust, while respecting applicable legal frameworks. In this context, while reaffirming the role of data for development, we highlight the work carried out in this topic by the Development Working Group during the Indian Presidency.

10. Acknowledging the growing demand and financing for DPI implementation in LMICs, we recognise the need for a comprehensive, multistakeholder approach with coordinated and voluntary financing and technical assistance, while ensuring adequate monitoring of progress and impact. We also acknowledge that the lack of adequate safeguards, sustained financing, and technical assistance can result in poorly developed DPI leading to several risks including data breaches and privacy violations, improper and unlimited access to personal data, violation of intellectual property rights, and security risks. In view of this, we underline the need to embrace global multistakeholder approaches, to build capacity, and provide technical assistance and adequate funding support for implementing robust, inclusive, human-centric, and sustainable DPI in LMICs. In this regard, we note the discussion initiated by the Indian Presidency on its proposal of the One Future Alliance (OFA), a voluntary initiative that aims to bring together governments, the private sector, academic and research institutions, donor agencies, civil society organisations and other relevant stakeholders and existing mechanisms to synergize global efforts in the DPI ecosystem.

11. We acknowledge the existing gap in information and knowledge sharing on DPI. To bridge this gap, we recommend strengthening ongoing efforts and building upon existing registries. Towards this, we welcome India's plan to build and maintain a Global Digital Public Infrastructure Repository (GDPIR), a virtual repository of DPI voluntarily shared by G20 members and beyond. The repository aims to share the practices and experiences of development and deployment of DPI which may include relevant tools and resources in different countries.

B. Building Safety, Security, Resilience and Trust in the Digital Economy:

12. Given the significant growth of the digital economy and the need for promoting safety, trust, reliability, resilience and protecting privacy and data, we affirm that

security in the digital economy is an increasing priority for all countries and stakeholders.

13. Under the 2017 German G20 Presidency, we acknowledged that trust and security were essential to harness the potential of the digital economy. These values were reaffirmed in 2018, 2019, and 2020 under the Argentine, Japanese, and Saudi Arabian G20 Presidencies, respectively. Further, during the 2020 Saudi Arabian G20 Presidency and 2021 Italian G20 Presidency, we recognised that security in the digital economy is a key enabling factor for sustainable development and growth. We continued the discussion under the Indonesian G20 Presidency in 2022 on the existing practices on digital security as a key enabler to support business continuity.

14. We recognise that digital solutions have become key enablers for service delivery in health, finance, education, manufacturing, public services, and utilities among other important sectors of the economy. Safety, security, resilience, and trust within the digital economy are vital to advance digital transformation and effectively harness the opportunities and address various challenges it presents.

15. We also recognise that global interconnectedness and digital dependencies across sectors and borders can create shared security risks associated with the digital economy that a single entity may not be capable of addressing alone. The digital economy has multiple layers, and, therefore, there is a risk that breaches or incidents at any layer may disrupt the functioning of the whole ecosystem. Due to the borderless nature of the digital environment, it is important for the G20 members and beyond to share their approaches and good practices to build a safe, secure, and resilient digital economy.

16. We acknowledge that preventing and mitigating security threats to the digital economy depends on stakeholders' capacities to understand, anticipate, prepare for, and respond to these threats. Therefore, we endeavour to further a common understanding of security risk management for the continuity of businesses, including Micro Small and Medium Enterprises (MSMEs), in the digital economy. To this end, we welcome the non-binding ***G20 High-Level Principles to Support Businesses in Building Safety, Security, Resilience, and Trust in the Digital Economy*** **(Annexure 2A)** which draw from the practices, strategies and tools developed and implemented by G20 members. These principles seek to strengthen resilience in the digital economy by promoting a culture of security, capacity building, multi-stakeholder cooperation and supporting research and development.

17. We recognise the potential risks associated with the digital economy and their impact on society, particularly children and youth. Considering that the digital environment opens new avenues for children and the youth to explore their creativity, enhance their learning experience, and work collaboratively, we acknowledge that the increased access to digital tools and services can increase exposure to a spectrum of risks to which children are especially vulnerable, such

as, cyberbullying and grooming, and child sexual abuse and exploitation as well as risks related to their personal data and privacy. We also recognise that women and girls are disproportionately affected by technology facilitated gender-based violence. In 2021, under the Italian G20 Presidency, we adopted High Level Principles for Children Protection and Empowerment in the Digital Environment. We reaffirm that cyber education and cyber awareness for the protection and empowerment of children and youth in the digital ecosystem, including protecting their best interests and respecting human rights in the digital environment continues to be one of our key priority areas.

18. We welcome the Indian Presidency's ***G20 Toolkit on Cyber Education and Cyber Awareness of Children and Youth[1] (Annexure 2B)*** that recognises the important role of the UN Convention on Rights of the Child and the need to develop holistic, human-centric approaches to address online safety across different jurisdictions which promote respect for and facilitate governments' efforts to protect children's privacy and personal data, uphold children's dignity, and respect their rights.

C. Digital Skilling for Building a Global Future Ready Workforce:

19. We recognise that the increasing digital skill gaps among our societies, economies and the workforce can be disruptive for the digital economy and result in increasing digital divides, particularly for women and girls. Therefore, we resolve to enhance our collective efforts to promote digital skills and digital literacy with a focus on addressing digital divides and skill gaps, including gender skill gaps, through skilling, reskilling, upskilling and other capacity building initiatives. In this regard, we reaffirm our support for the efforts made by the 2016 Chinese, 2017 German, 2018 Argentine and 2022 Indonesian G20 Presidencies. The 2023 Indian Presidency builds on the fourth pillar of the toolkit proposed by Indonesia, i.e., 'jobs' in the digital economy.

20. Supporting a gender equal workforce and the acquisition of digital skills ranging from basic to advanced are key to promoting inclusive and sustainable development. Designing and promoting inclusive education, training programs and other learning opportunities, particularly for underserved groups and people in vulnerable situations, can contribute to reducing the digital skill gap. Therefore, we recognise the importance of identifying the relevant skill sets and bridging the information gap between job seekers, employers, education and training institutions, and civil society actors.

21. Given that digital technologies are changing the skills needed for any job, we recognise the need to upskill and reskill the workforce with the relevant technical and socio-emotional, or transversal skills. The digital era also calls for the need to equip the workforce with skills to ensure human centric and privacy friendly design, development, and use of these technologies. We thus welcome the ***G20***

[1] The document "G20 Toolkit for Cyber Education and Cyber Awareness for Children and Youth" was produced by the Indian G20 Presidency and is based on the responses provided by the G20 members and guest countries to the Cyber Security Questionnaire circulated by the Indian Presidency. Annexure 2B contains a brief summary of this toolkit.

Toolkit for Designing and Introducing Digital Upskilling and Reskilling Programs[2] **(Annexure 3A)** which outlines an indicative strategy for the design and implementation of digital upskilling and reskilling programs. The toolkit further identifies a number of good practices related to the skilling, upskilling, and reskilling and serves as a resource to help better assess and improve strategies towards building a future-ready workforce.

22. We acknowledge that many G20 members have established taxonomies and endowment frameworks based on skills, occupations, professional certifications, or job roles. However, there is a lack of a widespread measurement of skills, abilities and competencies enabling cross-country comparisons, as observed during the G20 Argentine Presidency (2018). Therefore, we recognise that there is a need for a common understanding of digital skills across borders to potentially tap into a broader talent pool and help address the supply and demand gap of a digitally skilled workforce. We thus, welcome the ***G20 Roadmap to Facilitate the Cross-Country Comparison of Digital Skills*** **(Annexure 3B).** This roadmap is a series of broad steps that seeks to enable a common understanding of job roles, digital skills, and related credentials among G20 member states and beyond.

23. Based on voluntary engagements, we also recognise the value of the Indian Presidency's proposal to develop a virtual Centre of Excellence (CoE) which would be built and maintained by UNESCO as a repository of good practices on digital skilling initiatives, occupational standards, skill taxonomies, professional certifications, skill credentials, and studies related to demand and supply gaps, especially related to digital skills and would aim to exchange relevant information and encourage learning from interested countries' approaches.

D. Geopolitical Issues

24. This year, we have also witnessed the war in Ukraine further adversely impact the global economy. There was a discussion on the issue. We reiterated our national positions as expressed in other fora, including the UN Security Council and the UN General Assembly, which, in Resolution No. ES-11/1 dated 2 March 2022, as adopted by majority vote (141 votes for, 5 against, 35 abstentions, 12 absent) deplores in the strongest terms the aggression by the Russian Federation against Ukraine and demands its complete and unconditional withdrawal from the territory of Ukraine. Most members strongly condemned the war in Ukraine and stressed it is causing immense human suffering and exacerbating existing fragilities in the global economy – constraining growth, increasing inflation, disrupting supply chains, heightening energy and food insecurity, and elevating financial stability risks. There were other views and different assessments of the situation and sanctions. Recognising that the G20 is not the forum to resolve

[2] The document "G20 Toolkit for Designing and Introducing Digital Upskilling and Reskilling Programs" was produced by the Indian G20 Presidency and is based on the responses provided by the G20 members and guest countries to the Digital Skilling Questionnaire circulated by the Indian Presidency. Annexure 3A contains a brief summary of this toolkit.

security issues, we acknowledge that security issues can have significant consequences for the global economy.[3] [4]

25. It is essential to uphold international law and the multilateral system that safeguards peace and stability. This includes defending all the Purposes and Principles enshrined in the Charter of the United Nations and adhering to international humanitarian law, including the protection of civilians and infrastructure in armed conflicts. The use or threat of use of nuclear weapons is inadmissible. The peaceful resolution of conflicts, efforts to address crises, as well as diplomacy and dialogue, are vital. Today's era must not be of war.

Way forward

26. We affirm that our deliberations and outcomes on Digital Public Infrastructure for Digital Inclusion and Innovation; Building Safety, Security, Resilience and Trust in the Digital Economy; and Digital Skilling for Building a Global Future-Ready Workforce seek to advance our collective efforts to build an enabling, inclusive, open, fair, non-discriminatory, and secure digital economy. In the context of digital economy, we respect applicable legal frameworks. We also seek to foster a digital economy that promotes respect for human rights, privacy, and protection of personal data for all, and contributes to the implementation of the 2030 Agenda for Sustainable Development and achievement of Sustainable Development Goals.

27. We are grateful to all G20 members and guest countries for their contributions to the G20 Digital Economy Working Group (DEWG) under the Indian presidency. We would also like to thank the international organisations and our knowledge partners i.e., ITU, OECD, UNDP, UNESCO, and World Bank who contributed and provided valuable feedback towards achieving the outcomes.

28. Brazil, as the next Presidency of the G20, looks forward to building upon the achievements of past presidencies in order to continue to promote an inclusive, sustainable, development-oriented and human-centric approach, with the fundamental aims of realising the full potential of the digital economy for all, improving people's lives and bridging the digital divides. We therefore welcome Brazil's plans to work on the topics of universal and meaningful connectivity; artificial intelligence; information integrity and trust in the digital environment; and digital government.

29. We believe that the outcomes of this Ministerial meeting would be a useful resource and could continue to contribute actively to the work of future presidencies and work collectively to realise the benefits of the global digital economy.

*****

[3] Russia rejected the inclusion of geopolitical Para 24, on the basis that it does not conform to the G20 mandate and recognizes the status of the Para 24 as Chair's Summary. Russia agrees with the rest of the text.
[4] China stated that the G20 DEMM is not the right forum to discuss geopolitical issues and did not support the inclusion of the geopolitical-related content.

ANNEXURE 1

G20 FRAMEWORK FOR SYSTEMS OF DIGITAL PUBLIC INFRASTRUCTURE

1. Digital public infrastructure represents a promising approach towards digitalisation, which leverages a whole-of-society approach to provide benefits across sectors. Considering the diverse approaches of G20 members to digital transformation, we recognize that digital public infrastructure is an evolving concept that may not be limited to sets of digital systems with these characteristics and could be tailored to specific country contexts and can be referred to with different terminologies. Under the Indian Presidency's initiative, digital public infrastructure is described as a set of shared digital systems, the key idea behind which is designing minimal digital building blocks that can be used modularly by governments, businesses, academia, and civil society to enable society-wide development. The 'public' in digital public infrastructure can refer to public benefit and access, subject to appropriate governance and oversight by public authorities. We recommend consideration of the following elements in the development and deployment of these systems.

    a. Three components: technology, governance, and community.

    b. Suggested principles for (development and deployment).

2. This voluntary and suggested framework is developed as neutral reference that recognizes that choice of technology and models will be determined by country contexts.

a. THREE COMPONENTS: TECHNOLOGY, GOVERNANCE AND COMMUNITY

3. **Technology:** This comprises digital systems and applications (e.g., software codes, protocols, standards) that are interoperable. These building blocks provide a stand-alone, reusable service or set of services. They can be used flexibly for different use cases and sectors. These can be open source and/or proprietary solutions, as well as a combination of both.

4. **Governance:** Governance is critical in facilitating user adoption at scale by establishing trust. Governance frameworks may include rules of engagement governing stakeholder behaviour, cross-cutting and domain specific norms, laws and policies, and governance embedded into digital technologies (for e.g., privacy enhancing technologies). It provides safeguards, including those that promote respect for human rights and protection of personal data, privacy, and intellectual property, as well as accessible and transparent grievance redressal mechanisms. Governance frameworks may also include accountable institutions for maintaining oversight on its design, deployment, and implementation. It may also seek to ensure long-term funding to ensure sustained and uninterrupted operations.

5. **Community:** Vibrant and inclusive community participation can enable value creation. This also comprises private sector and civil society actors who can collaborate to unleash innovation and unlock value.

6. **SUGGESTED PRINCIPLES [5]: TECHNOLOGY, GOVERNANCE AND COMMUNITY**

   a. **Inclusivity:** Eliminate or reduce economic, technical, or social barriers to enable inclusion, empowerment of end-users, last-mile access, and avoid erroneous algorithmic bias.
   b. **Interoperability:** Enable interoperability by using and building on open standards and specifications with a technology neutral approach, wherever possible, while accounting for appropriate safeguards and keeping in view the legal considerations and technical constraints.
   c. **Modularity and Extensibility:** Extensible approach implies a building block or modular architecture to accommodate changes/modifications without undue disruption.
   d. **Scalability:** Use flexible design to easily accommodate any unexpected increase in demand and / or to meet expansion requirements without changing existing systems.
   e. **Security and Privacy:** Adopt an approach that embeds key privacy enhancing technologies and security features within the core design to ensure individual privacy, data protection, and resilience based on standards offering appropriate levels of protection.
   f. **Collaboration:** Encourage the participation of community actors at different stages of planning, designing, building, and operating to facilitate and promote a culture of openness and collaboration. Enable the development of user-centric solutions and facilitate widespread and sustained adoption and allow innovators to develop new services.
   g. **Governance for Public Benefit, Trust, and Transparency:** Maximise public benefit, trust, and transparency while respecting applicable legal frameworks. This means that laws, regulations, policies, and capabilities should seek to ensure that these systems are safe, secure, trusted and transparently governed, and also promote competition, and inclusion, and adhere to principles of data protection and privacy.
   h. **Grievance redress:** Define accessible and transparent mechanisms for grievance redress, i.e., user touchpoints, processes, responsible entities, with a strong focus on actions for resolution.
   i. **Sustainability:** Ensure sustainability through adequate financing and technological support and enhancements to facilitate uninterrupted operations and seamless user-focused service delivery.
   j. **Human rights**: Adopt an approach that respects human rights at every stage of the planning, designing, building, and operating.

[5] The aim of these Principles is to build upon the advancements in this domain, such as the Principles on Identification for Sustainable Development, the CPMI-IOSCO Principles for Financial Market Infrastructures, UN Principles for Responsible Digital Payments, and the Principles for Digital Development.

k. **Intellectual Property Protection:** Provide adequate and effective protection and enforcement of intellectual property rights for the rights-holders of technologies and other materials used based on existing legal frameworks.
l. **Sustainable Development**: Seek to develop and deploy these systems that contribute to the implementation of the 2030 Agenda for Sustainable Development and achievement of Sustainable Development Goals.

ENABLERS OF INNOVATION, GROWTH, AND INCLUSION

7. Leveraging digital technologies for economic activities often necessitates certain basic functions. These can include the ability to identify and authenticate individuals and businesses and secure and seamless flow of money and information. Digital public infrastructure can fulfil these core functionalities through interoperable digital systems, such as: digital ID, digital payment systems, and data sharing mechanisms with consent wherever applicable in line with the principles as described in Para 6 above. Some of these core functions are described below:
    a. Identification: The ability for people and businesses to securely verify their identity, as well as complementary trust services such as electronic signatures and verifiable credentials.
    b. Payments: Easy and instant transfer of money between people, businesses, and governments.
    c. Data sharing with consent wherever applicable: Seamless flow of personal data with consent, wherever applicable, across public and the private sectors, with safeguards for personal data protection as per applicable data governance frameworks.

8. Network effects of these systems can bring transformative changes in the digital economy as well as help countries achieve their developmental goals.

ANNEXURE 2

A. G20 HIGH-LEVEL PRINCIPLES TO SUPPORT BUSINESSES IN BUILDING SAFETY, SECURITY, RESILIENCE, AND TRUST IN THE DIGITAL ECONOMY

Recognising the importance of security in the digital economy and to support businesses, we endorse the following non-binding High-Level Principles to build safety, security, resilience, and trust in the digital economy:

1. **Security and Trust**

We seek to develop a human-centric culture of security and trust in the digital economy that enables citizens and businesses to understand risk management by:

a. Promoting cyber hygiene and the development of market-led and industry-led standards based on the principles of openness, transparency, and consensus.
b. Encouraging businesses and supporting MSMEs to develop and implement good practices and risk management frameworks to maintain the integrity of global supply chains.
c. Promoting a 'security by design' and phased risk management approach along with encryption measures for digital solutions and services, including in emerging technologies and connected systems and their devices.
d. Promoting resilience in connected sectors such as health, finance, manufacturing, and public services and utilities by taking suitable security measures.
e. Encouraging accessible and efficient grievance redressal mechanisms for businesses, MSMEs, and consumers that fall victim to malicious use of digital technologies.

2. **Capacity Building**

We acknowledge that capacity building is an important aspect of advancing security across the multilayered structure of the digital economy and should include:

a. Collaborating with and encouraging relevant stakeholders, including international organisations, to prioritise and contribute to capacity building within their areas of expertise.
b. Exploring an interdisciplinary approach that includes strategy, governance, technology, regulatory and non-regulatory frameworks, culture, economics, incident response and crisis management.
c. Providing guidance and awareness to citizens, businesses including MSMEs, and the wider economy on how to stay safe and secure online in an inclusive and accessible manner.
d. Promoting lifelong learning opportunities for all users of digital technologies.
e. Encouraging young people especially women and girls to consider a career in security of digital solutions and services through curricular or extracurricular programs.

3. **Research and Development**

We recognise the importance of advancing research and development to build

resilience by:

a. Promoting research in advanced and emerging technologies that can enhance protection against security threats.
b. Sharing best practices on how to tackle various security threats, including recommendations from international organisations.
c. Facilitating research projects on topics such as the economic costs of security incidents and their impact on businesses and underrepresented communities.
d. Promoting studies to measure security-related digital divides and its impact on economies.

4. **Multistakeholder Cooperation**

We recognise that partnering with businesses, civil society organisations, academia, international organisations and the technical community is key to promoting security in the digital economy and can be reinforced by:

a. Developing opportunities for public private partnership collaboration and engagement.
b. Supporting the sharing of trends on known and existing vulnerabilities faced by nongovernmental stakeholders in the digital environment.
c. Facilitating engagement between businesses and points of contacts across various industry incident response teams.

5. **Strengthening Resilience of Essential Services**

We recognise the importance of preventing damage or disruptions to certain essential social and economic services in the digital economy and encourage stakeholders to:

a. Take suitable measures to protect services essential to the digital economy from security threats.
b. Encourage businesses to set up mechanisms to assess the security of their supply chains for essential services in an evidence-based approach.

6. **Support for MSMEs in the Security Ecosystem**

We recognise the role of MSMEs in the digital economy and support strengthening the MSME security ecosystem by:

a. Driving innovation by supporting MSMEs that offer security solutions and services to scale-up and grow.
b. Providing guidance and support to MSMEs on how to operate securely in a digital environment.
c. Creating opportunities for MSMEs to engage with governments, shape policy approaches and share good practices to improve resilience to combat particular security challenges.
d. Seeking to mobilise additional cooperation, funding, and support for MSMEs to improve their security capacity.

B. TOOLKIT ON CYBER EDUCATION AND CYBER AWARENESS OF CHILDREN AND YOUTH

7. The close integration of digital technologies in the lives of children and youth has translated into various benefits, such as access to information, increased connectivity to online spaces, and the opportunity to learn a wide array of skill sets. However, as per the United Nations International Children's Emergency Fund (UNICEF) the surge in online activity has also led to a proliferation of cyber risks specifically targeting children and youth.

8. International organisations such as the ITU have recognized the significance of this challenge and framed guidelines such as the ITU's Guidelines on Child Online Protection, Guidelines for policymakers. The G20 members have explicitly acknowledged this challenge and opportunity. In 2021, the G20 Digital Economy Ministers committed to the non-binding G20 High Level Principles for Children Protection and Empowerment in the Digital Environment, which this toolkit builds upon.

9. The toolkit relied on three phases of research:

    a. Phase 1: Empirical desk-based research that reviewed a range of publicly available sources on G20 countries to map information relating to the core research questions.
    b. Phase 2: Consultation with G20 members and obtaining direct insights through a questionnaire circulated in February 2023.
    c. Phase 3: Consolidation of data from mapping and consultation.

10. To mitigate these risks, G20 members and guest countries have adopted and implemented a broad range of measures. These include comprehensive regulations and capacity-building measures, such as the creation of dedicated websites and applications. This toolkit has recorded some of these measures. We found that measures to further child online safety are based on a combined assessment of the following factors:

    a. The type of risk
    b. Targeted actor
    c. Implementing stakeholder
    d. Desired outcome

11. This toolkit depicts this approach in a pyramidal model but acknowledges that the adopted measures may vary from this approach as per the social, economic, political and cultural contexts of a member.

12. Drawing from desk research and responses to a survey circulated by the Indian Presidency among all the G20 members and guest countries, the toolkit shares five takeaways that policymakers may consider while developing cyber education and cyber awareness initiatives for children and youth. These include:

a. Classifying risks and responses based on sub age groups.
b. Investing in response, referrals, and support systems.
c. Adopting and investing in a multi-stakeholder approach throughout the decision-making process.
d. Promoting global cooperation to further child online safety.
e. Recognising the critical role of businesses and online platforms.

ANNEXURE 3

A. G20 TOOLKIT FOR DESIGNING AND INTRODUCING DIGITAL UPSKILLING AND RESKILLING PROGRAMS

1. Digital transformation and new technological developments are changing the way we live, work, and behave, deeply transforming economies and societies worldwide. Projections point to important shifts in the workforce due to use of automation and artificial intelligence technologies, both in terms of possible job losses and change in job profiles and job tasks. Digital skill gaps, including among women and girls, emerge as the key factor hampering technological development and adoption.

2. Formulation of comprehensive digital skill development strategies can contribute to inclusive digital economies. We further recognise the need for basic and advanced digital skills, and associated socio-emotional or transversal[6] skills, in addition to skills related to the responsible design, development, and deployment of digital technologies, for a future ready, gender equal, inclusive workforce.

3. Addressing this need, we have developed the **G20 Toolkit for Designing and Introducing Digital Upskilling and Reskilling Programs** to help the design and implementation of digital upskilling and reskilling programmes at scale. This toolkit builds on the fourth pillar of the toolkit proposed by the Indonesian G20 Presidency in 2022, i.e., 'jobs' in the digital economy.

4. The G20 Toolkit for Designing and Introducing Digital Upskilling and Reskilling Programs serves as a compendium of good practices, enabling factors, implementation challenges, and case studies of successfully implemented digital skilling programmes across G20 members and other countries. The toolkit further delineates an indicative and flexible strategy which can be referenced when developing and deploying digital skilling programmes.

5. The structure of the **G20 Toolkit for Designing and Introducing Digital Upskilling and Reskilling Programs** is as follows:

a. Compendium of Digital Skilling Initiatives

The compendium reflects the responses received to the questionnaire circulated among G20 members and guest countries. It consolidates information provided by G20 members and guest countries on aspects including skill qualification frameworks, occupational standards, as well as programmes, strategies, and schemes for digital skilling. It highlights examples of stakeholders' collaboration, mechanisms for credentials and certifications, enabling factors and challenges faced by members in their initiatives, and shares key lessons learnt. The case studies presented in this section reflect successful actions or initiatives deployed by G20 members and guest

[6] According to UNESCO, transversal skills are those typically considered as not specifically related to a particular job, task, academic discipline or area of knowledge but as skills that can be used in a wide variety of situations and work settings (IBE 2013). These skills are increasingly in high demand for learners to successfully adapt to changes and to lead meaningful and productive lives. Examples include- Critical and innovative thinking, Interpersonal skills, Intrapersonal skills, Global Citizenship, Media Literacy.

countries.

b. Indicative Strategy for Designing and Introducing Digital Skilling, Upskilling and Reskilling Programmes

The compendium is complemented by an indicative strategy for the introduction of digital upskilling and reskilling programs. The strategy draws from the initiatives and experiences of G20 members and guest countries and may be followed or built upon flexibly by the governments of G20 members and beyond. The proposed strategy entails:

i. Identifying key relevant emerging technologies to build a future-ready, gender equal workforce.

ii. Classifying job tasks and mapping them to required digital skill sets and job tasks to assess upskilling and reskilling needs for current and future workforce.

iii. Assessing gaps in existing digital skilling programmes to improve design and implementation.

iv. Leveraging short-term training in addition to school and higher education curricula, to keep pace with technological developments and market needs.

v. Investing in trainers and faculty to improve their training capacity in digital skills and enable the use of innovative digital technologies in pedagogy.

vi. Developing and promoting an ecosystem of digital credentials for easier verifiability, accessibility, and comparability.

B. ROADMAP TO FACILITATE CROSS COUNTRY COMPARISON OF DIGITAL SKILLS

6. To address the need for a widespread measurement of skills, abilities and competencies enabling cross-country comparison already highlighted by the Argentine Presidency in 2018, the **'Roadmap to Facilitate Cross Country Comparison of Digital Skills'** encourages countries to identify, define, and compare digital skills and competencies across borders, while also promoting workforce development in the digital economy. It seeks to establish a common understanding between taxonomies related to the skills needed for the digital era, with the aim to contribute to greater employment, innovation, and economic development.

7. The 'Roadmap to Facilitate the Cross-Country Comparison of Digital Skills' builds on existing skills recognition frameworks. Given the diversity of approaches to recognising skills in different countries, the roadmap has been envisioned as a series of broad steps, for countries to flexibly adapt the roadmap to their specific contexts. The roadmap can facilitate the engagement of countries in bilateral or

multilateral dialogues to help create a common understanding of the digital skills needed in different job roles, in addition to tasks, qualifications, and credentials or professional certifications.

8. By facilitating collaboration, the roadmap can help devise a coordinated approach to respond to digital skill demands by different industries. It seeks to help countries identify emerging digital skills and needs, prioritise investments in relevant areas, and inform upskilling and reskilling policies undertaken by governments and industry.

Key Considerations for Cross-country Comparison

9. While countries may have different approaches when it comes to recognising digital skills, common elements emerge. These relate to accessibility of information, comparability, evidence, and verifiability, which all represent elements enabling more effective comparisons of digital skills across borders.

10. Access to comprehensive information about the digital skilling syllabus, content, learning and proficiency can enable better understanding of individuals' digital skills, knowledge, and experience, enabling effective comparison.

11. Comparability enables the assessment and comparison of digital skill credentials, qualifications, experience, and proficiency across countries, ensuring that digital skills can be evaluated and acknowledged consistently.

12. Evidence in the form of documented proof of digital skill credentials is essential for comparison of digital skills. This may include professional certifications, or any other credentials that provide tangible evidence of an individual's digital skills.

13. Verifiability establishes the legitimacy of digital skill credentials and enables trust among stakeholders.

14. It is important to note that these considerations are not exhaustive, and countries may use any, or all of these, as a basis for cross country comparison.

Key Components of the Roadmap

15. The roadmap comprises the following components:

    a. **Identification and classification of knowledge, skills, and competencies in the digital era:** In order to effectively perform a particular job, or task, it is important to identify the knowledge, skills, and competencies required for the digital era. These encompass digital, technical, and socio-emotional / transversal skills to enable responsible design, development, and use of technologies[7].

[7] In line with UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021)

b. **Measurement and assessment of proficiency:** The knowledge, skills and competencies identified need to be assessed in terms of the level of proficiency required. The criteria related to such assessment may be shared, to facilitate comparison, benchmarking, and good practices.

c. **Establishing suitable similarities[8]:** Participating countries may collectively identify similarities in relation to skills, especially digital skills, qualifications, job roles and tasks, as well as required proficiency levels, and credentials.

d. This process would enable **assessment and comparison of digital skills** across educational or professional systems to inform the design and implementation of upskilling and reskilling programmes and policies, in support of industry and employment outcomes.

[8] 'Similarities' refers to any metric (s) that a country may choose to use while comparing digital skills, competencies, credentials in another country.