B20 India Secretariat
Confederation of Indian Industry

B20 INDIA 2023

R.A.I.S.E.

Responsible
Accelerated
Innovative
Sustainable
Equitable

TASK FORCE ON

Digital Transformation

Policy Paper

TASK FORCE ON

Digital Transformation

Policy Paper

Published by

Confederation of Indian Industry (CII)
The Mantosh Sondhi Centre; 23, Institutional Area,
Lodi Road, New Delhi 110003, India

Contents

Foreword: Leadership of the Task Force

RAJESH GOPINATHAN
Co-Chair,
B20 India Task Force on Digital Transformation and
Former MD & CEO, TCS Ltd.

ROSHNI NADAR MALHOTRA
Co-Chair,
B20 India Task Force on Digital Transformation and Chairperson,
HCL Tech Ltd.

The theme for B20 under India's Presidency is - R.A.I.S.E – Responsible, Accelerated, Innovative, Sustainable, Equitable Businesses (and business practices). Digital Transformation plays a central role in achieving such business practices.

Today we stand at the precipice of an unprecedented digital revolution, where the boundaries of innovation are expanding at an astonishing pace. The role of Digital Transformation has become more critical than ever, shaping the trajectory of nations and industries alike.

The global economy has been propelled by the tremendous growth and integration of digital technologies. Estimates show that the global digital economy contributes to more than 15% of the global GDP and in the past decade, it has grown 2.5 times faster than the physical world GDP. Despite the growth, we must acknowledge that there are existing gaps that hinder progress– (i) Heterogenous network connectivity and quality still leave many people unconnected, (ii) the quality of digital education varies widely, leading to significant gaps in digital literacy levels of individuals and hampering the seamless movement of talent, (iii) Micro, Small and Medium enterprises still face barriers in the adoption of digital, and (iv) Increasing frustration with the overall digital ecosystem, with the rising cost of cybercrime despite ever-increasing complexity of regulatory compliance.

Our mission as the B20 Digital Transformation Task Force is to address these challenges head-on, driving actionable solutions to foster global digital inclusion. We believe that empowering businesses and individuals with future-proof universal connectivity, digital literacy, tools, and resources for digital adoption and greater cooperation in the area of cybersecurity, will enable them to not only participate but also thrive in the digital economy.

We are committed to the goal of unlocking the full potential of the digital economy in regions around the world, through our recommendations to the G20 leaders. Together, we must ensure that no one is left behind in this journey towards a digitally transformed society.

Let us strive to build inclusive societies that leverage the power of technology to unlock human potential, fuel innovation, and foster sustainable economic growth.

The time for action is now.

Messages from Co-Chairs

"Digital literacy serves as the foundation for successful digital transformation, emerging as a crucial skill in the 21st-century. Despite the pressing need, global disparities in digital skills persist, with definitions and frameworks varying across countries. Harmonising and setting standards for digital education and skills development are vital to empower individuals and drive economic development in the digital era. This must be accompanied by accurate measurement of digital skills, to identify gaps and guide policymakers, educators, and organisations in bridging these divides. Together, we must pave the way for an inclusive, future-ready society and ensure that no one is left behind."

KARAN BHATIA
VP, Government Affairs & Public Policy, Google

"The shift towards digitisation has revolutionised how businesses operate and how individuals work. As we continue to embrace new technologies, it is evident that this process of technological advancement will persist indefinitely and that digital inclusion, particularly for MSMEs, must be a fundamental part of resilient digital transformation. Through focus and collaboration, we can ensure that digital innovation benefits the entire economy."

DANIEL BRYANT
EVP, Global Public policy and Government Affairs, Walmart Inc.

"With connectivity, foundational to digital transformation, governments should speed the deployment of high-performing, affordable networks and ensure everyone has the skills for the digital age. India leads by example, leveraging connectivity to deliver its 'Digital India' program to its citizens."

Börje Ekholm
President and CEO, Ericsson

"To increase inclusion and tackle inequality, we need to achieve universal broadband connectivity as fast as possible. Incentivising investments, reducing cost of deployment and increased public-private sector collaboration are all required to accelerate digital infrastructure rollouts, which will help bring economic and education opportunities and healthcare access to more people. The sooner we close the connectivity gap, the quicker digitalisation across industries will deliver improved productivity, safety, and sustainability."

PEKKA LUNDMARK
President and CEO, Nokia Corporation

"The rapid expansion of digital technologies during the pandemic has brought forth unparalleled growth opportunities. However, to ensure the longevity of this digital advantage, it becomes crucial to prioritize the establishment of resilient infrastructure and a safety net that safeguards its usage. This policy paper serves as a progressive stride towards fostering inclusive growth through Digital Transformation. Achieving success in this endeavor necessitates a steadfast commitment from both the government and industry to seamlessly integrate digital tools into our economy and create pathways for those currently excluded from the digital realm."

LUIS MOSQUERA
VP and General Counsel Brazil, Siemens AG

"During pandemics, the world, especially SMEs which are hit the hardest, have learned to adapt to survive. Digital transformation provides SMEs with tools to survive by giving them instant access to customers, suppliers, and all stakeholders across the value chain. This transformation shall continuously be implemented to realise the full potential of the digital economy. The Digital Transformation Task Force have developed policies to accelerate digital transformation adoption by addressing the gap in the internet accessibility, digital infrastructure, digital security, digital literacy, and favourable regulatory environments."

FAJRIN RASYID
Director of Digital Business, PT Telkom Indonesia (Persero) Tbk

"Digitalisation is critical for transforming all sectors of the economy and holds immense promise for individuals and society as a whole. We must unleash the potential of digital transformation, placing it at the forefront of government and industry agendas. This means creating an environment that guarantees widespread access to modern connectivity, fosters investment in infrastructure and promotes open markets to ensure equal opportunities for all."

JOAKIM REITER
Chief External and Corporate Affairs Officer, Vodafone

"In today's digital landscape, trust holds immense significance, encompassing policies in digital security, data protection, and intellectual digital assets. Digital trust has become a foundational element for all stakeholders, and the G7 Hiroshima Leader's Communique in 2023 highlighted operationalising DFFT (Data Free Flow with Trust) and a major key to the future while multi-stakeholder engagement is highly expected. Our paper aims to shed light on the future of cyberspace, emphasising the importance of raising awareness about cyber-safety, establishing norms to protect data as a value creating business resource, and equipping businesses, especially MSMEs, to enhance cyber-preparedness and supply chain resilience including cross border market. Taking these transformative steps will bring about a significant shift in ensuring a secure future for all."

MAKOTO YOKOZAWA
Co-Chair, Committee for Digital Economy Policy, Business at OECD (BIAC)

Recommendations: Executive Summary

Recommendation 1 – bridge the digital divide by accelerating universal, future proof, and transformational connectivity across all regions and communities to increase digital penetration, drive sustainable investment, and deliver inclusive growth

Policy action 1.1: Ensure access to high-quality, modern, and reliable internet through fixed, mobile, and satellite broadband systems by improving the investment climate and implementing suitable reforms to incentivise the private sector, removing deployment barriers, securing the availability of affordable spectrum with optimum license duration, and ensuring a predictable, transparent, technology-neutral regulatory environment that encourages fair competition, global standards, and interoperable systems

Policy action 1.2: Complement and amplify private sector efforts along the entire value chain to boost internet affordability and accessibility by leveraging targeted and technology-neutral public interventions, including inclusive and innovative financing schemes for networks, services, and devices and a balanced approach to taxation to ensure the widespread deployment and adoption of transformational connectivity

Recommendation 2 – address digital literacy and skill gaps by developing global minimum standards for digital literacy to enable international skills portability, creation of an inclusive and diverse workforce and global measurement of digital literacy levels

Policy action 2.1: Institutionalise a global body to achieve the mandate of setting unified standards and metrics for digital literacy by adopting a global competence framework, sharing best practices, accrediting institutions and teachers trained under the framework, and operationalising the guidelines for developing learning material, curriculums, and assessments through multi-stakeholder and cross-national partnerships

Recommendation 3 – promote enterprise transformation for Micro, Small, and Medium Enterprises (MSMEs) through access to sustainable finance, a globally recognised and sector-specific digital toolkit, and a favourable regulatory environment

Policy action 3.1: Expand efforts to provide sustainable financing to MSMEs for adopting digital technologies and complementary services

Policy action 3.2: Establish a globally recognised digital toolkit and framework supported by a favourable regulatory environment that enables the creation of a digital ecosystem and provides end-to-end support to MSMEs in their digital transformation journey with a focus on creating a user-friendly and accessible platform that caters to the needs of MSMEs of different sizes and industries

Recommendation 4 – promote digital trust by developing harmonised cybersecurity standards and frameworks and bridging the cybersecurity skill gap, while fostering greater multilateral cooperation around cyberspace and enabling wider trust around digital systems and processes

Policy action 4.1: Institutionalise a global body with a mandate of harmonising and advocating cybersecurity standards and bringing in a greater degree of multilateral cooperation for shared goals of cyber action

Policy action 4.2: Improve the trustworthiness of the digital ecosystem and work towards a cyber-inclusive future by advocating cyber-awareness till the grassroots level

Policy action 4.3: Bridge the cybersecurity skill gap by facilitating the faster development of a cyber talent pipeline through increased investment in existing cyber-skilling institutes, complemented by building National Cyber Academies, through the public-private partnership route

Introduction

The significance of data as an economic and strategic resource is increasing rapidly and is further strengthened by changes induced by the pandemic. Especially at a time when inter-regional and international businesses were on lockdown, cross-border data communications and international business links based on them played a catalytic role in maintaining and growing the economy. Governments and businesses across the globe dealt with pandemic-induced disruptions by relying heavily on digital innovation. Digital technologies have transformed manufacturing, services, trade, and the whole society by bringing in greater efficiency and creating new ecosystems. There has been enormous growth in internet use, spurred by the COVID crisis. As per the International Telecommunication Union (ITU)[1], ~5.3 billion people or 66% of the world's population were estimated to be using the internet in 2022, an increase of 6.1% over 2021. Internet penetration across countries still varies widely. While more than 60% of the population in the Arab states and Asia-Pacific countries use the internet, only approximately 40% in Africa and 36% in the UN-designated Least Developed Countries (LDCs) and Landlocked Developing Countries (LLDCs) are online. Internet connectivity has been vital in helping maintain business continuity and the provision of all citizens' services. While universal connectivity is the first step in enabling digital transformation, having a digitally skilled population is equally important in ensuring appropriate use of the internet and other applications. The dominance of digital platforms on all stages of operations in the value chains has been gaining traction and the level of preparedness in navigating the digital era has quickly become a critical lever for driving the next phase of growth.

The evolving digital economy is characterised by big data handling and intelligent processing pools which can be analysed and scrutinised to feed into systems where Artificial Intelligence (AI), Machine Learning (ML), Generative Pretrained Transformation (GPT), and automated decision-making can be used to enhance and drive the entire digital ecosystem. A combination of emerging technologies such as AI, big data, Internet of Things (IoT), metaverse/immersive technology, distributed ledger technology, quantum technology, and Machine-to-Machine (M2M) are being used to further extend research and are being adopted across enterprises. The big data and AI market is expected to reach ~USD 4.5 trillion by 2025 and IoT is projected to unlock value of USD 15 trillion for global GDP by 2025[2]. The benefits of e-commerce and digital trade can also be leveraged to vitalise SMEs by structurally increasing their market access across borders and improving productivity.

Digital technologies, underpinned by transformational connectivity, can enable reductions in carbon emissions across the economy. Digital tools like big data analytics and ML can help to better understand energy demand and mobility choices which can in turn provide the basis for digital solutions for smart mobility options and energy networks[3]. The Exponential Climate Action Roadmap[4] underscores the potential of digital technologies to reduce global carbon emissions by up to ~15%. This can strongly support in achieving the overall 40% reduction target by 2030, set by many countries in reference to the United Nations Framework Convention on Climate Change (UNFCCC) and the Paris Agreement. Furthermore, ITU[5] estimates that Information and Communication Technologies (ICT) can help accelerate progress towards every single one of the 17 UN Sustainable Development Goals (SDGs).

Though digital transformation augments new opportunities for addressing developmental challenges and well-being creation, it also intensifies current concerns, such as enhanced access to and sharing of data, data protection, cybersecurity, disinformation/misinformation, and digital fraud. In 2021[6], the average number of

1 ITU, Measuring digital development Facts and Figure, 2022, https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/
2 Gartner, 2021
3 World Bank, Catalyzing Green Digital Transformation, 2022
4 World Economic Forum, Digital technology can cut global emissions by 15%. Here's how, 2019, Exponential Roadmap Initiative, 2020
5 ITU, Dec 2021, https://www.itu.int/en/mediacentre/backgrounders/Pag-s/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx
6

cyberattacks and data breaches increased by 15% from the previous year. Global cybercrime costs are estimated to hit USD 8 trillion in 2023 and reach USD 10.5 trillion by 2025[7]. The current regulatory environment for the protection of data is fragmented with the legal framework to protect data being outdated, insufficient, or incompatible in many cases. In both developed and developing economies, the enforcement of privacy and security obligations is often inadequate and not upto speed with rapidly advancing technological developments and fragmentation of regulations that vary from country to country. Furthermore, many developing countries still lack data protection and privacy legislation.

To realise the full potential of the digital economy, challenges with respect to gaps in internet accessibility, affordability, quality infrastructure, digital security, and digital literacy need to be addressed. A coherent and internationally interoperable digital legislation can bridge this digital divide through digital initiatives that provide equal access to all while adhering to the required privacy and cyber security norms.

The Antalya Summit in 2015 marked the first Communique in B20 that addressed the issue of digital trade, but without any delineation of a specific trade aspect of the digital agenda. In 2016, the Digital Economy Development and Cooperation Initiative was launched at B20 to promote tangible steps towards financial inclusion by embracing digital technologies. The Hamburg Summit (B20 Germany) in 2017 introduced digitalisation as a new priority area, wherein the importance of digital financial inclusion was highlighted by the leaders under the digitalisation Task Force. Ever since, the B20 has been focusing on various aspects related to global connectivity, digital inclusion, data flow and security, industry 4.0, AI, the digital gender divide, etc. At the 2019 B20 Tokyo Summit, the key recommendations covered data utilisation, cybersecurity, digital transformation, trusted AI utilisation, and the launching of real-world projects.

B20 Italy in 2021 iterated their commitment to unleash the potential of digital transformation as the driver for recovery post the pandemic. The deliberations focused on fostering a digitally ready and inclusive society, reducing connection inequalities, and promoting trust in the digital ecosystem. The Indonesian Presidency in 2022 focused on three priority issues for the Indonesian government, namely Global Health Architecture, Digital Transformation, and Energy Transition.

While digital transformation has taken a top spot on leaders' agenda for several years, the crisis has accelerated its urgency. In a post-pandemic world, companies cannot go back to business as usual. Future competitiveness and resiliency will depend on maximising the value from digital transformations[8].

Building on the previous presidencies and their recommendations, the key objectives for Digital Transformation Task Force under India presidency are:

- **Strengthening digital infrastructure availability and reach:** Promoting future-proof connectivity by ensuring network capacity and reach and providing quality connections.
- **Accelerating digital adoption:** Building digital literacy to enable digital inclusion and user empowerment and addressing skill gaps through reskilling and upskilling of the workforce.
- **Empowering MSMEs to scale and transform digitally:** Making enterprises, especially MSMEs, more digitally savvy and sustainable, fostering innovative and locally adapted services for customers.
- **Promote digital trust and address the cybersecurity skill gap:** Developing harmonised cybersecurity standards and frameworks, strengthening existing cyber skilling institutes while fostering greater multilateral cooperation around cyberspace and enabling wider trust around digital systems and processes.

7 Cybersecurity Ventures, Official Cybercrime Report 2022

8 BCG, Leaders path to digital value, 2021

Recommendation 1

Bridge the digital divide by accelerating universal, future-proof, and transformational connectivity across all regions and communities to increase digital penetration, drive sustainable investment, and deliver inclusive growth

Policy actions

1.1 Ensure access to high-quality, modern, and reliable internet through fixed, mobile, and satellite broadband systems by improving the investment climate and implementing suitable reforms to incentivise the private sector, removing deployment barriers, securing the availability of affordable spectrum with optimum license duration, and ensuring a predictable, transparent, and technology-neutral regulatory environment that encourages fair competition, global standards, and interoperable systems

1.2 Complement and amplify private sector efforts along the entire value chain to boost internet affordability and accessibility by leveraging targeted and technology-neutral public interventions, including inclusive and innovative financing schemes for networks, services, and devices and a balanced approach to taxation to ensure the widespread deployment and adoption of transformational connectivity

Leading Monitoring KPI	**Owner: G20 Countries**	
Percentage of people connected to the internet	Baseline **66%** (2022)	Target **75%** (2025)

Source: International Telecommunication Union (ITU)

Recommendation 1 contributes to the achievement of UN's SDG 5: gender equality, SDG 8: decent work and economic growth, SDG 9: industry innovation and infrastructure, SDG 10: reduced inequalities, and SDG 17: partnership for the goals

Policy action 1.1 contributes to better work standards and economic growth by solving connectivity issues across geographies. Improving connection quality has a positive impact on GDP, contributing to target 8.1 and 8.2 in sustaining per capita GDP and technological upgradation and innovation. Fostering technological empowerment and connectivity development supports the accomplishment of SDG 9, specifically 9.b as well as industry value and internet penetration in 9.c. It also directly ties to indicator 9.c.1 "Proportion of population covered by mobile network". Increasing connection reach would benefit indicator 17.6.1 "Fixed internet broadband subscriptions over 100 inhabitants by speed" as well as indicator 17.8.1 "Proportion of individuals using internet". By granting the same level of connectivity in urban and rural areas and reducing inequalities in technology access, it would also benefit target 10.1, sustaining income growth of the bottom 40% of the population.

Policy Action 1.2 amplifying private sector efforts to boost internet affordability, supports SDG 17 – SDG 17.7 which ties to promoting and developing new forms of technology across countries and SDG 17.8 which is meant to fully operationalise the technology bank for developing countries. It also supports SDG indicator 17.7.1, which measures "Total amount of funding for developing countries to promote the development, transfer, dissemination, and diffusion of environmentally sound technologies". Further, it supports SDG 5.b.1 "Proportion of individuals who own a mobile phone, by sex" as it covers policy actions on device affordability and gender equity.

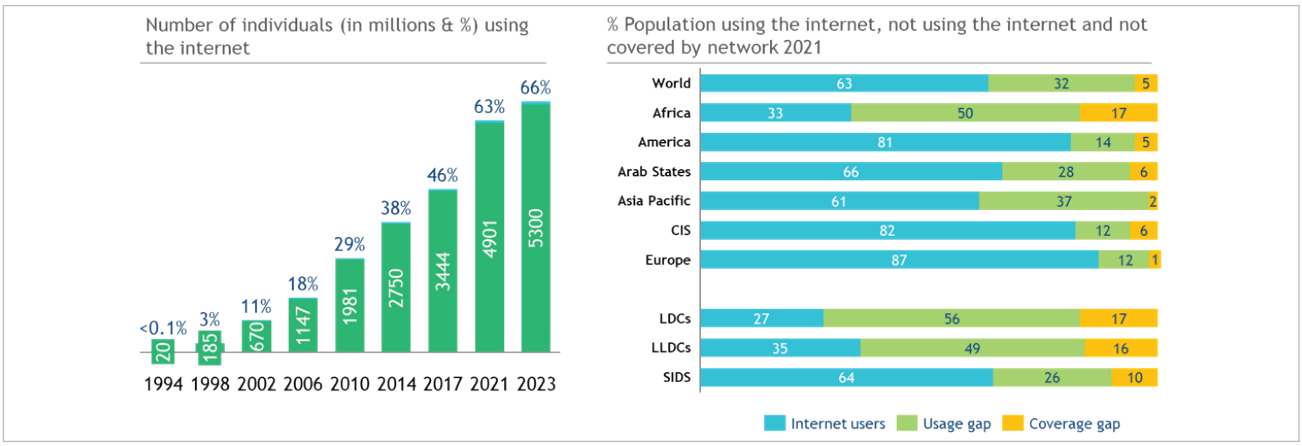
CONTEXT

In this section, we lay out the connectivity landscape in terms of coverage, quality of connection, and changing demand patterns followed by key barriers to internet adoption.

High-performing, high-capacity connectivity is foundational for enabling digital transformation. Data is the lifeblood of digital transformation and connectivity allows this lifeblood to flow - it enables data to flow through network infrastructure to reach citizens. The share of the population that can use the internet has been rising globally, with a steep increase in recent years. As a matter of fact, ~5.3 billion people or 66% of the world population was using internet in 2022, a rise from ~4.9 billion (or 63% of the population) in 2021[9]. This has been led by higher internet penetration, and not just by mere high population growth.

In 2021, 37% of the global population was not using the internet. Out of these 37% people, 5% had a 'coverage gap', i.e., they lived in an area not covered by a broadband network while 32% had a 'usage gap', i.e., they lived within the footprint of a broadband network but were not using internet services (Refer Exhibit 1). This indicates that while a large proportion of people had access to the network, they were not able to use it. This effect was more pronounced in LDCs and LLDCs – 56% and 49%, respectively. In 2022, given that the percentage of people not using the internet had declined to 34%, we can assume that the other gaps followed the same trend across regions. As per ITU report 2022, 36% of people in LDCs are using the internet (up from 27%).

Exhibit 1: Rising proportion of internet users alongside gaps in coverage & usage



Source: International Telecommunication Union (ITU)

Note: The coverage gap is the percentage of the population that does not have access to a mobile or fixed network.
The usage gap is the percentage of the population not using the Internet minus the coverage gap.

It has been observed that there is a significant relation between broadband penetration and countries' GDP growth - a 10% increase in fixed broadband penetration drives 0.77% growth in GDP per capita while a similar increase in mobile broadband penetration yields 1.5% growth in GDP per capita[10]. A study conducted for Africa[11] shows that for every 10% increase in mobile broadband penetration, there is an average GDP increase of 1.8% and 2% in middle-income and low-income countries, respectively. It is predicted that the latest generation of connectivity, 5G, could add USD 1.3 trillion to the global GDP by 2030[12]. Further, there exists a close relationship between digital connectivity and human development (Refer Exhibit 2).

Exhibit 2: Relationship between connectivity and human development

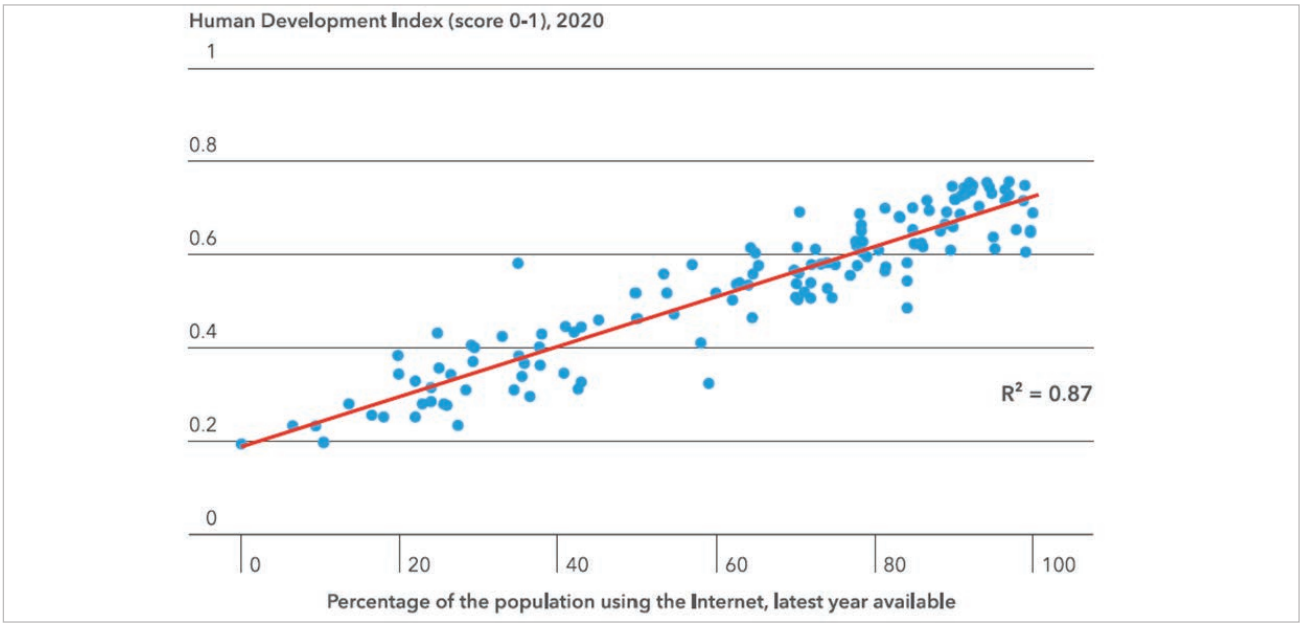


Figure 1.1: Connectivity and human development

Source: International Telecommunication Union (ITU)

Note: N-138

9 ITU, Measuring digital development Facts and Figure, 2022, https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/

10 ITU, The economic impact of broadband and digitisation through the COVID-19 pandemic Econometric modelling, 2021 https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.COV_ECO_IMPACT_B-2021-PDF-E.pdf

11 ITU, Economic contribution of broadband, digitisation and ICT regulation Econometric modelling for Africa,2019, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDT_A-FR-2019-PDF-E.pdf

12 PwC 2021

Despite rising connectivity, ~2.7 billion people are still offline, more than 90% of whom live in developing countries. Regional disparities (Refer Exhibit 3) show that Africa is the least connected region with ~60% of the population (~67% in 2021) offline followed by Asia-Pacific (36%) and the Arab states (30%) in 2022. Connectivity issue is majorly in LDCs, especially for women, where ~70% women are still offline. The share of internet users also varies in urban-rural areas: users are estimated to be twice (~1.8) as high in urban areas as in rural areas. This contrast is more pronounced in Africa where the urban to rural internet user ratio is 2.8, down from 4 in 2019. This gap is also pronounced across different age groups. Globally, it is estimated that 75% of the youth (15-24 years of age) use the internet while 65% of the other age groups are using the internet[13]. There is disparity in individuals owning a mobile phone as well – 58% in LDCs (vs global average of 73%).

About one in seven persons or more than a billion people around the world identify themselves with a disability, hence making them the largest minority group. Global statistics about the connectivity status of people with disabilities does not exist. Data collected by GSMA for some middle-income countries indicates significant gaps between people with disability and those without it, separating them at each stage of the mobile internet user journey, right from mobile ownership and awareness to adoption and usage. For instance, in Algeria, the smartphone ownership gap extends to ~50% and internet use gap extends to ~40%[14].

The digital divide is further widened due to a difference in the level of technical capabilities in each country. Developed countries have more advanced technological infrastructure and higher digital maturity and skills which allows them to develop and implement newer and more efficient technologies, thereby further widening the gap. We can also say that the usage gap is more pronounced on account of linguistic barriers. Mobile devices, which are the most common medium to go online, are available in very few languages. Additionally, the lack of diverse content in multiple languages further widens the adoption gap.

Exhibit 3: The global digital divide – global disparity of internet use share

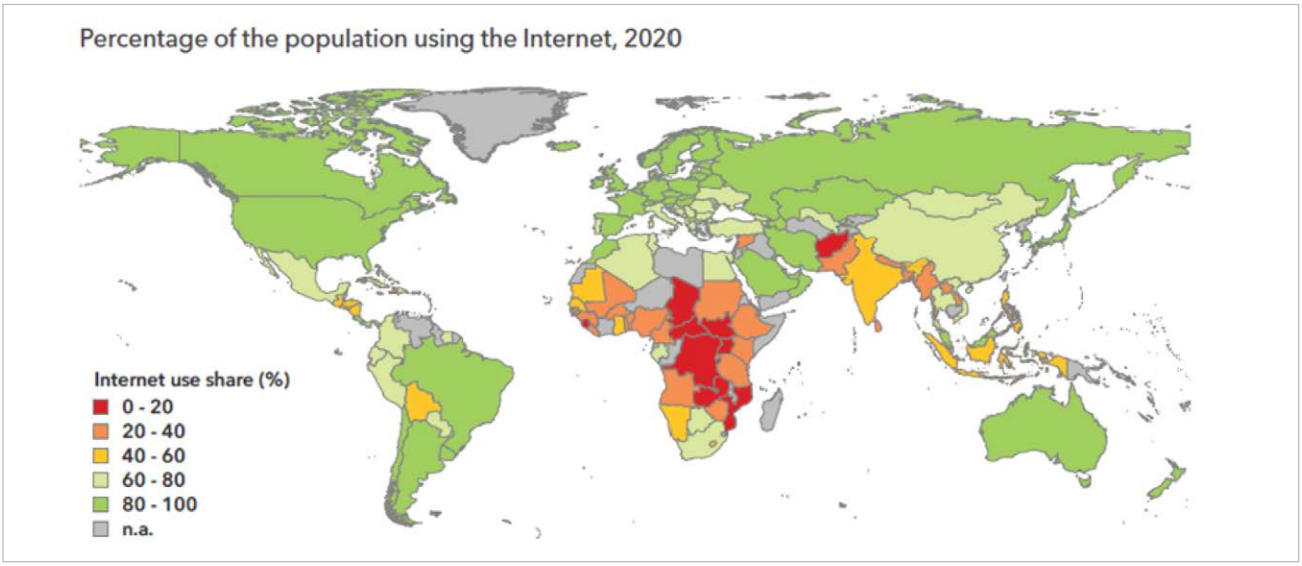


Figure 2.5: The global digital divide

Source: International Telecommunication Union (ITU)

Note: The designations employed and the presentation material on the map do not imply the expression of any opinion whatsoever on the part of ITU, concerning the legal status of the country, territory, city or area or its authorities, or concerning delimitation of its frontier boundaries. The base map is the UN map database of the UN Cartographic Section.

13 ITU Facts and Figures 2022, Global Connectivity Report, 2022

14 ITU: Global Connectivity Report, 2022

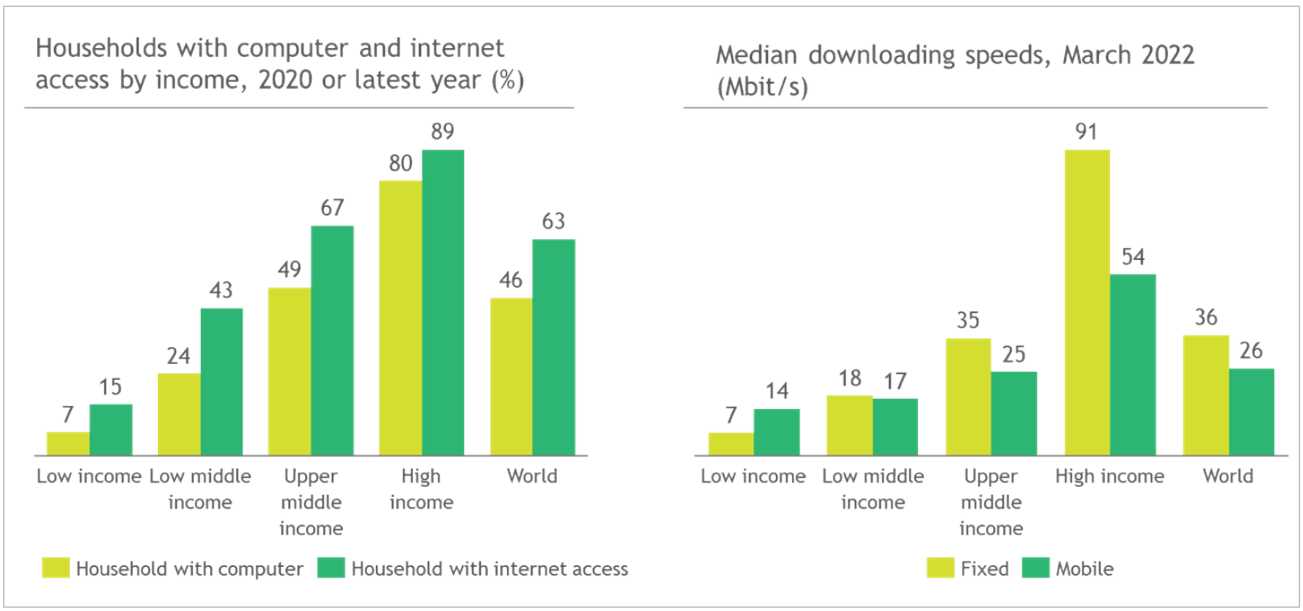
Despite the recognised importance of connectivity, the quality of networks and their coverage varies drastically. Even in cities that have internet, certain zones are less served than others. Many households with poor-quality broadband internet access rely on a mobile-broadband connection at home, which is often inadequate for data-intensive activities, such as remote schooling and teleworking. Only 63% of households around the world has internet access and less than half have a computer[15] (Refer Exhibit 4).

Apart from heterogeneity in the availability of network, there is also variability in the quality of connection, such as capacity and speed. As per ITU's Facts and Figures Report 2022, while international bandwidth usage has increased by 25% in 2022, wide variations on a per-user basis continue to persist globally. For instance, in Europe, the international bandwidth usage per user (~397 kbit/s) is 5x times the bandwidth usage per person in Africa (~85 kbit/s).

There are wide differences in median download speed performance depending on income group and region. As Exhibit 4 shows, the median downloading speed for fixed internet in High-Income countries is ~13x the speed in low-income countries. Further, for mobile, it is ~4x.

Around 40-44% of people in low and middle-income countries are not using mobile internet despite being covered by a mobile broadband network. This can partially be attributed to the poor quality of connection, which impacts access to critical services, such as remote education and virtual healthcare.

Exhibit 4: The global digital divide – households with computer and internet access (%), 2020 or latest available data



Source: ITU/UNESCO, State of Broadband 2022 (speeds via Ookla)

Connectivity has become more critical post-pandemic as a majority of interactions in work, education, and social life, which previously took place offline, have moved online post-pandemic. During the pandemic, the underlying infrastructure faced unprecedented demand – the demand for broadband communication services increased as the use of virtual communication tools rose by 10 times while online streaming increased by more than 50% all around the globe[16]. IXPs (bulk traffic exchange points where multiple networks connect to exchange traffic) reported an increase of 60% in

15 Broadband Commission for Sustainable Development, The State of Broadband 2022: Accelerating broadband for new realities, 2022

16 Nielsen, COVID-19 Tracking the Impact on Media Consumption, 2020

total bandwidth handled per country[17]. The increased use of digital content will further drive network demand. As the world increasingly moves online, the impact of digital divide between people with and without access to quality internet is expected to become even more striking.

Despite the accelerated increase in demand, the adoption of internet has been uneven. As per GSMA consumer survey[18], there are multiple barriers to internet adoption and use. These include:

- **Access:** Lack of access to networks and enablers such as internet-enabled handsets, devices, and services which are either not accessible or not easy to use
- **Affordability:** Inability to afford devices, data plans or service fees
- **Knowledge and skills:** Lack of digital skills and literacy accompanied with limited awareness and understanding of mobile internet and its benefits
- **Relevance:** Lack of relevant content, products, and services that meet users' needs and capabilities
- **Digital trust:** Concerns about the negative aspects and risks of internet such as theft, fraud, etc.

The B20 would like to urge governments to focus on universal and meaningful connectivity – defined as the possibility for everyone to enjoy a safe, satisfying, enriching, productive, and affordable online experience – which has become the new imperative in the 2020-2030 Decade of Action[19]. To achieve the same, the B20 Digital Transformation Task Force would like to draw attention to two priority areas:

- **Policy action 1.1:** Ensure access to high-quality, modern, and reliable internet through fixed, mobile, and satellite broadband systems by improving the investment climate and implementing suitable reforms to incentivise the private sector, removing deployment barriers, securing the availability of affordable spectrum with optimum license duration, and ensuring a predictable, transparent, and technology-neutral regulatory environment that encourages fair competition, global standards, and interoperable systems
- **Policy action 1.2:** Complement and amplify private sector efforts along the entire value chain to boost internet affordability and accessibility by leveraging targeted and technology-neutral public interventions, including inclusive and innovative financing schemes for network, services, and devices and a balanced approach to taxation to ensure the widespread deployment and adoption of transformational connectivity

Policy Action 1.1: Ensure access to high-quality, modern, and reliable internet through fixed, mobile, and satellite broadband systems by improving the investment climate and implementing suitable reforms to incentivise the private sector, removing deployment barriers, securing the availability of affordable spectrum with optimum license duration, and ensuring a predictable, transparent, and technology-neutral regulatory environment that encourages fair competition, global standards, and interoperable systems

In order to bridge the infrastructure gap, the G20 should focus on the effective implementation of National Broadband Plans (NBPs), continuous roll out of fixed and mobile broadband, and promote competition and investment in new wireless and emerging technologies. This should be accompanied by an overall improvement in the investment climate, removal of deployment barriers, and a fair regulatory environment, which includes technology-neutral interventions, forward-looking spectrum policy, and a level playing field across the digital value chain.

17 OECD, Keeping the internet up and running in times of crisis, 2020, https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/

18 GSMA, The State of Mobile Internet Connectivity 2022

19 ITU: Global Connectivity Report, 2022

1. The G20 should promote the effective implementation of NBPs across all countries and operationalise "Broadband for all" by 2025

The Broadband Commission for Sustainable Development[20] requires all countries to have funded National Broadband Plan or strategy or include broadband in their universal access and services definition by 2025. These plans are policy documents defining the goals and aspirations of the country's ICT sector over the medium and long term and are crucial to increasing meaningful access[21] within the countries. They are essential for promoting transparency and assigning clear roles and responsibilities to all in order to ensure that different stakeholders fairly contribute to the implementation of "Broadband for all", thereby fostering collaboration and improving citizens' accessibility to technology. Transparency and clarity help operators to optimise network planning and reduce capital expenditure, putting them in a better position to invest in and deploy their networks.

The number of countries with NBPs has decreased from 165 in 2021 to 155 in 2022[22] as plans have expired or haven't been renewed. While plans have been established in many countries, challenges in implementation continue to persist. For example, countries which have called on the use of Universal Service and Access Funds to deploy infrastructure have encountered problems such as poor design, mismatch between collections and disbursements, etc.

Existing NBPs need to be strengthened across multiple dimensions:

a. **Coverage aspiration** viz, a roadmap for the implementation of newer technologies, such as 5G (how will it be introduced, the services that might be offered, timescales for preparatory work to plan for spectrum release, etc.), lay out the network penetration roadmap prioritising both geographical areas and communities with low connectivity, define key enablers for achieving these targets, such as infrastructure requirements (e.g., digital subscriber lines, fiber optic network, wireless networks), establish investment policies, etc.

b. **Solidify implementation enablers,** e.g., on-ground operational guidelines, empower relevant authorities for outcome orientation, provide the right funding models, especially from an execution standpoint, etc.

2. The G20 should ensure technology and vendor neutrality so that the most suitable products and solutions are quickly developed and deployed to meet the complex and evolving connectivity needs of countries and communities

Governments should take a technology and vendor neutral approach when facilitating infrastructure deployment along the entire value chain of the internet - development of core networks, spectrum provision, construction and installation of infrastructure, provision of devices, etc. Technologies, such as fixed cable, fiber optic cables, and 4G/5G connection might, for example, often be better suited in a plain terrain and high-population density, urban and metro cities, whereas technologies such as fixed wireless access and satellite broadband might be more appropriate in remote geographies with poor terrain and low population density rural and hilly areas.

2a. The G20 should focus on improving the network availability and reliability by facilitating continuous broadband expansion of fixed and mobile services, wherever feasible, as well as alternate wireless technologies, to provide high-quality internet

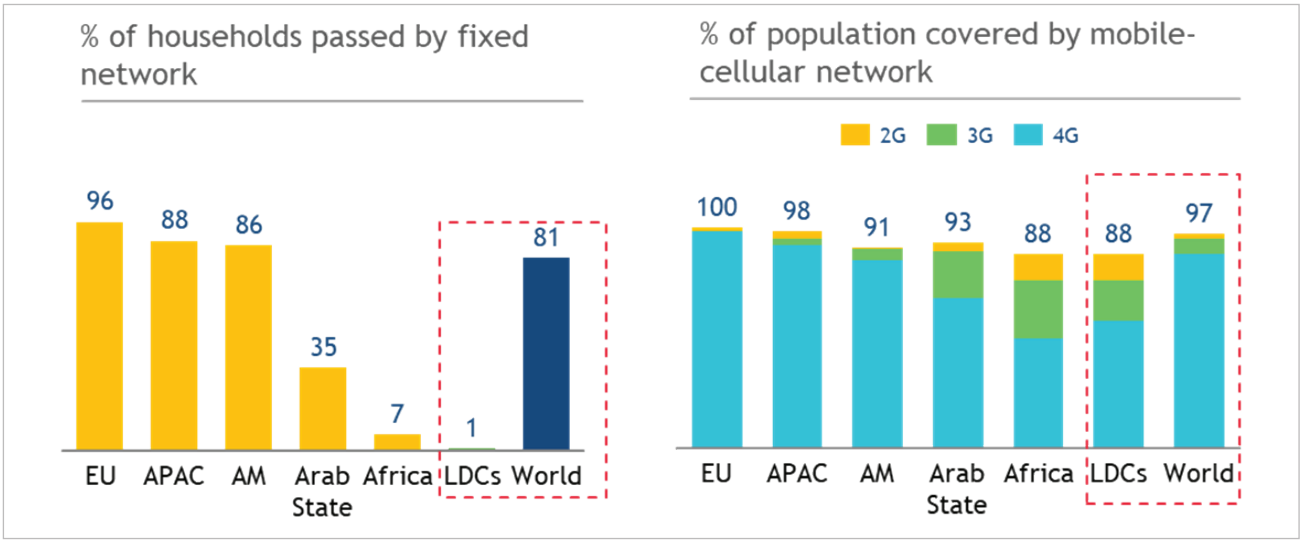
Governments should facilitate the continuous roll out of fixed and mobile broadband services in areas where connectivity is feasible. But a vast majority of people do not have access to fixed networks due to their location. For a household to access a fixed network, a last-mile connection is needed to bring the network home. Only 1% of households in LDCs can access a fixed network (Refer Exhibit 5). For rural/remote areas which face a unique set of challenges associated with the delivery of high-speed broadband, including geographical variables and high costs, alternate options should be considered.

20 Commission is a PPP that was established in 2010 by ITU and UNESCO as a UN advocacy engine to boost the importance of broadband on the international policy agenda and expand broadband access to every country

21 Broadband Commission for Sustainable Development, Global Goal of Universal Connectivity Manifesto, 2020

22 Broadband Commission for Sustainable Development, https://www.broadbandcommission.org/advocacy-targets/1-policy/

Exhibit 5: Coverage based on fixed vs mobile network



Source: ITU

Depending on geographical conditions, internet service providers can encounter difficult terrains which makes planning and executing a fixed buildout difficult. At the same time, the population density of the rural market is low while the construction cost of fixed network is high – both these factors make it challenging for providers to recover their investment, thereby restricting rural broadband.

The Government can help in the provision of fixed broadband through better civil planning in synergy with broadband investments. It can also explore alternate wireless technologies which can deliver high-quality internet at a lower cost for areas with low feasibility of fixed and mobile broadband services. Fair and efficient market competition among market players should be encouraged to enable investment in infrastructure, provisioning of new services, and service improvements in quality (in terms of faster speeds and coverage).

2b) The G20 should encourage the participation of technology companies offering innovative solutions through satellite systems to strengthen network deployment in areas with poor connectivity

The satellite sector has rapidly expanded and gone through significant changes in recent times with the number of space launches increasing by 32% in 2022 to 2,553 objects[23]. Satellite operators are expected to create a more competitive environment for the provision of rural and semirural broadband which will help to connect the unconnected in the future. New broadband satellite systems are being developed that are technically more complex than earlier stationary satellites. These satellites offer wider coverage, greater capacity, and lower latency than was previously available. However, it is more complex for them to agree on how to operate their networks without causing harmful interference to each other, which could cause localised degradation to the quality and reliability of these services. Several companies are developing these systems and regulators should look at enabling more to provide services to increase choice in the market.

Various companies are adopting a range of different network architectures and business models. So it is crucial that approaches and regulatory frameworks maintain vendor neutrality and promote fair market competition. Alongside, it should be ensured that the deployment of these systems are done in an environmentally sustainable way, taking into account the investments already made by existing players and ensuring that the use of satellite systems does not contribute to the digital divide by creating a two-tiered internet where certain users have access to higher-quality internet than others.

23 ISRO (Indian Space Research Organisation), Indian Space Situational Assessment for the year 2022, 2023, https://www.isro.gov.in/Indian_Space_Situational_Assessment_2022.html#:~:text=Global%20Scenario&text=In%202022%2C%20more%20space %20objects,inserted%20in%20orbit%20were%20witnessed.

3. The G20 should incentivise private sector network investment by facilitating fair competition and removing deployment barriers to facilitate infrastructure build out

Governments can facilitate network build out and coverage by improving the investment climate and championing fair competition. This can be achieved by ensuring technology and vendor neutrality, where governments avoid picking winners (companies or technologies) and thus, distorting markets and impinging on investment. Fair competition and a level playing field spurs investment, innovation, and cooperation.

Direct government interventions should be limited to market failures alone and in helping meet the needs of underserved households and businesses, again without distorting competition dynamics and in a way that amplifies private sector investments, while respecting technology neutrality.

Governments should also support network deployment by fostering transparent and efficient permit granting procedures. The rollout and deployment of 5G needs to happen at greater speed for countries, consumers, and industries everywhere to reap the benefits of technology innovation.

The fast deployment of telecommunications infrastructure such as base stations and masts should be encouraged. This includes national-level guidelines to facilitate the acquisition of new sites, e.g., lamp posts, traffic signals, etc., to accelerate small-cell deployments, as well as streamline planning processes to avoid lengthy deployment delays and facilitate site upgrades. The fees to use public sites should be on a cost recovery basis to accelerate deployment.

An open environment should be encouraged where operators can share infrastructure with other industries, for example, fiber networks used by utilities or alongside railways, public sites for towers, etc., to reduce the cost and accelerate the deployment of 5G, especially in underserved areas. The faster the deployment barriers are removed, the quicker society connects and reaps broader, socio-economic and environmental benefits.

4. G20 countries should establish a technology neutral regulatory environment that encourages global standards, optimises spectrum license duration, and provides internet access in a fair and competitive manner

4a. G20 should provide harmonised spectrum in a timely and affordable manner, focusing on harnessing long-term societal value

Spectrum – the finite number of radio waves allocated for communication over the airwaves - is a scarce natural resource that should be assigned to optimise long-term value to the economy and society. The G20 should focus on establishing a forward-looking spectrum policy that includes the timely release of spectrum, with licensing conditions that incentivise investments in broadband coverage and capacity. Additionally, licenses should require a period long enough to provide the certainty of tenure necessary to make investments in capacity and coverage.

In the short term, spectrum for 5G should be made available in the low, medium, and high bands, at affordable rates, prioritising the benefit of 5G for society. This would allow operators to invest in building a high-performing network for consumers and industries. Spectrum harmonisation of both frequency allocations and technical conditions is key for device ecosystem and economies of scale.

The spectrum policy should involve a range of licensing approaches to give flexibility, provided that the chosen approach can be shown to create the greatest social welfare. Spectrum fees can also be traded off for deployment objectives. In China and Japan, the governments trade-off spectrum fees for deployment commitments to ensure that the market delivers the connectivity output desired by policymakers. Governments should make licensed spectrum available on a flexible use and technology-neutral basis and not dictate technologies/architectures to be used - let the market decide the best technology and most appropriate use cases for each asset.

Further, governments should promote partnerships that lead to multi-stakeholder coordination and cooperation, which is the key to network infrastructure development plans. Accelerated network extension is contingent on enabling faster approvals for private-sector players to execute civil works, coordination between infrastructure players (e.g., road construction & telecom utilities) to prevent re-work and laying of optical fiber during road construction, setting up telecom towers, etc.

4b. The G20 should promote global, open standards to boost affordability and interoperability

The mobile industry's ability to grow and infinite advances in network efficiency would not have been possible without 3GPP[24] global standards which have allowed mobile technologies to compete, succeed, and scale globally, resulting in the expansion of mobile communication technology coverage to regions not previously covered.

Scale drives affordability. Due to the economies of scale, standards enable cost reduction for the entire supply chain including manufacturers, operators, and users. Global standards enable portability of mobile numbers and apps globally. For the benefit of all, countries should seek to prevent the fragmentation or bifurcation of standard setting for telecommunications and digital technologies.

Countries should avoid mandating country or region-specific standards that could distort the market and jeopardise product interoperability and consumer experiences. Indeed, countries should pursue the continuation of and adherence to global open standards as is the case with 5G, extending to 6G (3GPP).

5. G20 countries should facilitate setting a minimum broadband speed standard for countries to adopt, which also enables easier application for DPI, without it becoming a barrier for investment in areas where no access presently exists

Significant disparity exists around the definition of broadband speed across countries. India has defined a minimum download speed of 2Mbps to qualify as broadband, while other countries have different definitions. For example, Bangladesh has defined 5 Mbps, UK has defined 10 Mbps, and the USA has defined 25 Mbps as broadband. Some regions like the European Union[25] do not have a standardised minimum definition for broadband speed levels, however, they have a goal of providing 100 Mbps download speed for every household by 2025. Hence, the definition of broadband substantially varies across countries.

Digital public goods are becoming open-source and interoperable and require minimum internet speed to access various use-cases. For example, video KYC would require a minimum speed of 1-6 Mbps and watching training videos (Standard and High Definition) would require a speed of 3-8 Mbps[26]. The inequity around speed definitions across countries restricts wider access and adoption of these digital applications.

G20 countries should come together to define a minimum broadband speed standard so that network providers adhere to these common set of standards and provide quality internet access which will enable the wider adoption of digital public goods. This should not, in any case, become a barrier that prevents investment in connectivity solutions where no access presently exists.

Policy Action 1.2: Complement and amplify private sector efforts along the entire value chain to boost internet affordability and accessibility by leveraging targeted and technology neutral public interventions including inclusive and innovative financing schemes for network, services, and devices and a balanced approach to taxation, to ensure the widespread deployment and adoption of transformational connectivity

1. The G20 should promote the modernisation of USFs including coverage of newer technologies which are contextualised to area-specific connectivity needs and create regulatory frameworks to enable technology neutrality along with transparency and accountability in their delivery

24 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organizations known as "Organizational Partners" providing their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. 3GPP specifications cover cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications.

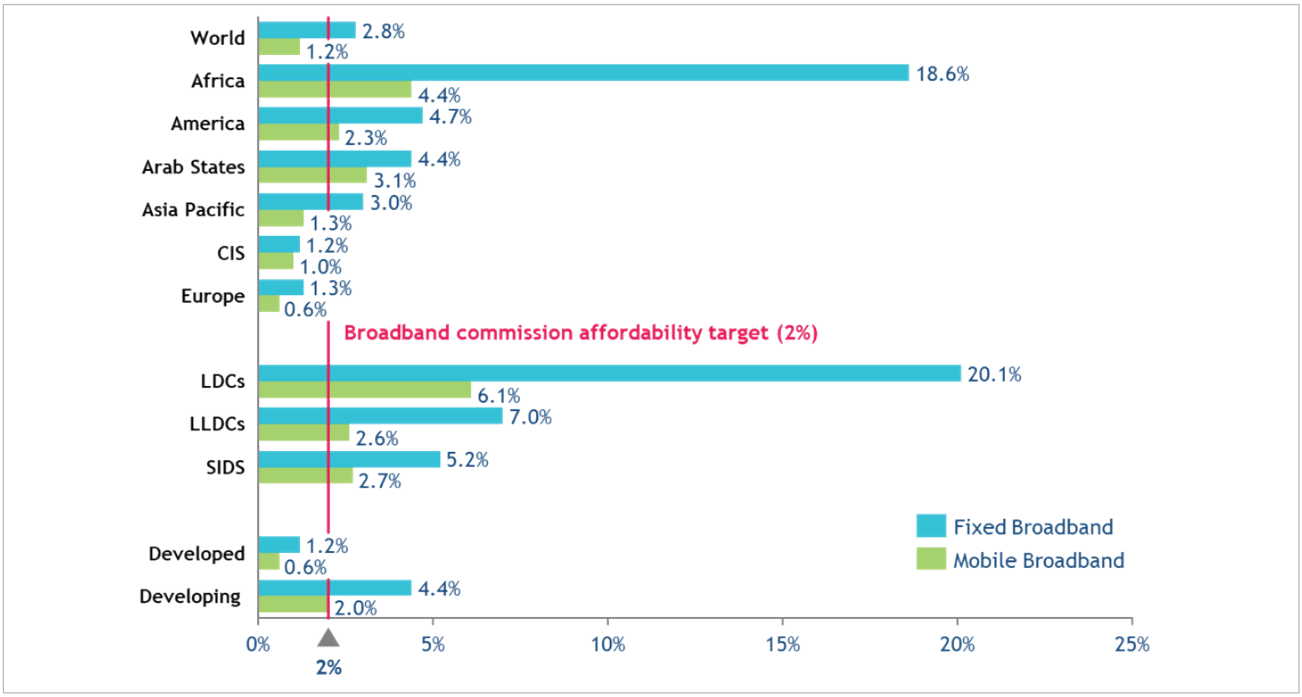
25 Fair Internet Report, July 2023, https://fairinternetreport.com/eu-broadband-definition

26 Federal Communications Commission, Broadband Speed Guide, July 2023 https://www.fcc.gov/consumers/guides/broadband-speed-guide

The UN Broadband Commission defines affordability target for internet accessibility as[27] - "By 2025, entry-level broadband services should be made available at less than 2% of monthly Gross National Income (GNI) per capita". Currently, the target is not met for most of the countries.

On average, mobile broadband has become more affordable in LDCs (~6% of monthly GNI) and LLDCs (~7% of monthly GNI), albeit still being distant from the goal. Comparatively, fixed broadband services are available at ~19% of GNI in LDCs (Refer Exhibit 6).

Exhibit 6: Fixed and mobile broadband basket prices, as a % of Gross National Income, 2020



Source: ITU

The Affordability Drivers Index (ADI)[28] is a tool developed by the Alliance for Affordable Internet (A4AI)[29] to assess how well a country's policy, regulatory, and overall supply-side environment is working to lower industry costs and create more affordable broadband. Countries with a higher score on the index have lower costs of connectivity. Since 2016, the ADI scores have risen only by 3.6% on an annual basis, in spite of policy scores increasing by 5%+ per annum. This indicates an underwhelming impact in Low-and-Medium-Income Countries (LMICs) to the changes in policy, underscoring the need to do more. Further, International Telecommunications Union (ITU) estimates that an additional investment of USD 428 billion will be required to connect the world by 2030[30].

Universal Service Funds (USF)[31] are funding mechanisms established by national governments to promote universal access to digital services including telecommunication services, broadband connectivity, and digital devices. They are collected through different mechanisms, such as annual regulatory fee, percentage of the telecom operators' gross or net annual revenue, contributions by international financing institutions, such as the World Bank, or directly from the national government's budget. They are then reallocated through subsidies and investments on projects for underserved areas.

27 Broadband Commission for Sustainable Development, 2025 Targets
28 Alliance for affordable internet, Affordability report 2021, https://a4ai.org/report/2021-affordability-report/
29 The Alliance for Affordable Internet (A4AI) is a global coalition working to drive down the cost of internet access in low- and middle-income countries through policy and regulatory reforms.
30 Alliance for affordable internet, Affordability Report, 2020
31 UNESCAP, The Impact of Universal Service Funds on Fixed-Broadband Deployment and Internet Adoption in Asia and the Pacific, 2017

USFs have been an effective catalyst in driving down the cost of connectivity and expanding coverage. Though several countries have established USFs, many have failed to disburse them effectively due to legal constraints or lack of regulatory frameworks to enable fund allocation[32]. Hence, governments should re-think USFs both from a scope as well as an execution point of view.

The G20 should promote the modernisation of USFs by scaling existing and proven technologies and business models and reorienting them towards new technologies, which work in a complementary fashion to traditional fixed-line networks and can expand the reach in currently underserved areas. Additionally, the technology funded by USFs should be contextualised to area-specific connectivity needs and archetypes, and not be a single, one-size-fits-all solution. Governments should also ensure that the technology is sustainable, resilient, and future proof. Countries should create regulatory frameworks to enable the transparent disbursement of funds and commit adequate resources (e.g., political coordination) to USF to deliver on its mandate.

2. The G20 should focus on improving device affordability through a balanced approach to taxation and a mix of inclusive and innovative financing models and multi-lateral agreements, with a focus on reducing gender, regional, and other disparities

As mobile access is the primary driver of connectivity, device affordability is the ability of an end user to pay for digital devices[33]. It is defined as the ratio of the handset device price and a person's income. It is a significant constraint for people who find the cost of handset/devices and access high and do not perceive sufficient value for money from going digital. There are multiple policy considerations to reduce the cost of handsets and improve access to finance.

Some of these include:[34]

- Re-evaluate sector-specific taxes (levied on top of VAT and custom duties in LMICs)
- Envisage different financing options which provide flexible payment terms for underserved customers, e.g., buy now, pay later, alternative credit risk, micro-payments, etc.
- Introduce handset subsidies for targeted user groups such as female entrepreneurs from low-income groups
- Establish refurbished phones business models and local handset manufacturing
- Enable public private partnerships to de-risk handset financing.

Further, emerging new technologies, such as remote handset locking and lightweight Operating System (OS) are now driving down the cost of handsets. Remote handset locking technologies enable providers to offer finance without credit scoring and use handset as a collateral. In 2020, Google, in partnership with Safaricom in Kenya, launched its device locking app which enabled customers to buy a smartphone in instalments under the Lipa Mdogo financing plan. In case of non-payment, the phone could be locked remotely, restricting access to mobile internet and calls/SMS.

Governments can also forge partnerships with the mobile industry to plan handset affordability initiatives and define a clear strategy for identifying beneficiaries. For example, a leading telecom player participated in Bhamashah Yojana scheme (direct benefit transfer scheme) in India, introduced by the Rajasthan Government, through which millions of phones were distributed to women.

In addition to affordability, governments should also consider data privacy and protection when subsidising devices. Governments must balance cost with the risks of highly extractive mobile devices – those that capture excessive amount of user data in exchange for a lower cost – to ensure data privacy and protection of end consumers.

32 A4AI, Universal Service And Access Funds In Latin America & The Caribbean, Dec 2021

33 GSMA, Making internet-enabled phones more affordable in low and middle-income countries, 2022

34 GSMA, Making internet-enabled phones more affordable in low and middle-income countries, 2022

Recommendation 2

Address digital literacy and skill gaps by developing global minimum standards for digital literacy to enable international skills portability, the creation of an inclusive and diverse workforce, and global measurement of digital literacy levels

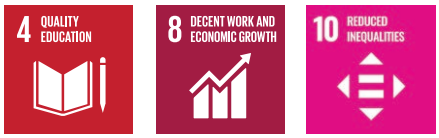
Policy actions

2.1 Institutionalise a global body to achieve the mandate of setting unified standards and metrics for digital literacy, adopting a global competence framework, sharing best practices, accrediting institutions and teachers trained under the framework, and operationalising the guidelines for developing learning material, curriculums, and assessments through multi-stakeholder and cross-national partnerships

Leading Monitoring KPI	**Owner: G20 Countries**	
Percentage of Individuals with basic, intermediate, and advanced digital skills[35]	Baseline **Basic: 55%** **Intermediate: 40%** **Advanced: 7%** (2022)	Target **Basic: 60%** **Intermediate: 45%** **Advanced: 10%** (2025)

Source: International Telecommunication Union (ITU), OECD data collected on SDG Indicator 4.4.1

35 SDG Indicator 4.4.1 "Percentage of youth and adults with ICT skills, by level" for OECD countries, as calculated in May 2023 using database from https://www.oecd.org/education/education-at-a-glance/EAG2022_X3-A.pdf



Recommendation 2 contributes to the achievement of UN's SDG 4: quality education; SDG 8: decent work and economic growth; and SDG 10: reduced inequalities

Policy action 2.1 ties to establishing digital literacy standards which are addressed by target 4.4 "By 2030, substantially increase the number of youth and adults who have relevant skills including technical and vocational skills, for employment, decent jobs, and entrepreneurship" which will be measured by indicator 4.4.1 "Proportion of youth and adults with information and communications technology (ICT) skills, by type of skill".

Policy action 2.1 calls for the reform of education curricula with the aim of including the digital skills required to address the needs of the forthcoming digital workforce, contributing to the same target. Ensuring the creation of a competent digital workforce in the future to support the achievement of targets 8.5 "By 2030, achieve full and productive employment and decent work for all women and men, including for young people and persons with disabilities, and equal pay for work of equal value". Finally, Policy Action 2.1 calls for the urgency of ensuring equal access to digital and technology trainings to all, covering target 10.2 aimed at empowering and promoting social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status".

CONTEXT

Digital literacy is the first step to successful digital transformation. As per UNESCO[36], digital skills are defined as a 'range of abilities to use digital devices, communication applications, and networks to access and manage information'. They enable people to create and share digital content, communicate, and solve problems. Digital skill gap existed even before the pandemic as the demand for digitally skilled workers was high across all levels of skills. However, as many jobs moved online during the pandemic, the skill gap has further widened. As per WEF[37], 41%+ companies believe that the 'skill gap' is one of the perceived barriers in digital adoption and is likely preventing companies from using digital services to their full potential.

Digital literacy has emerged as a critical life skill and is part of the 21st-century toolkit, as per WEF. In lower-income countries, only 32% of the population has basic digital skills (defined as the ability to copy or move a file or send e-mails). In higher-income countries, this number is around 62% and drops to 44% if standard skills (defined as the ability to use basic formula in a spreadsheet or create electronic presentations) are considered, which creates high barriers to adopting the required digital services to enable a remote lifestyle [38].

Digital literacy and skilling go hand-in-hand. While literacy is built out at a primary, secondary, and tertiary education level, digital skills come into play at workforce level. Digital skills also have different levels of complexity. Evidence shows that 30 economies have 40-60% population with basic ICT skills while only 4 economies have 80-100% population with basic ICT skills. This number becomes even lesser for advanced ICT skills – 35 economies have up to 5% population with advanced ICT skills whereas only 6 economies have 15-50% population with advanced ICT skills.

36 UNESCO, Digital Skills Critical for Jobs and Social Inclusion. As of 18 August 2021: https://en.unesco.org/news/digital-skills-critical-jobs-and-social-inclusion

37 World Economic Forum, Future of Jobs, 2020

38 WEF X BCG, Accelerating Digital Inclusion in the New Normal, Playbook 2020

Analysis indicates that by 2028, G20 countries could miss out on a projected USD 11.5 trillion uplift[39] to cumulative GDP if the digital skills gap is not proactively addressed. This translates to losing approximately 1.1% of GDP growth (over the 14 countries measured) with China (1.7%) and India (2.3%) at the greatest GDP growth risk.

According to WEF, we need to reskill more than 1 billion people by 2030. In order to thrive in a digital economy, a combination of digital and multi-disciplinary skills will be needed. The top skill groups that employers see as rising in prominence in the lead-up to 2025 include groups such as critical thinking and analysis as well as problem-solving in addition to skills in self-management such as active learning, resilience, stress tolerance, and flexibility[40]. These skills also facilitate the effective use of digital technologies. Additionally, it will become imperative to train the workers on the advancing technologies such as AI, automation, robotics, IoT, etc., and their applications in industries.

As countries and businesses evolve digitally, a vast majority of existing work tasks within traditional jobs will be modified. Data suggests that a large number of companies expect to restructure their workforce in response to new technologies. A forecast in 2020 estimated that 32% of all jobs in OECD countries are at significant risk of automation[41]. Evidence shows that 39% workers are concerned about not getting sufficient training in digital and technology skills from their employer[42].

It has already been established that there exists a digital skill gap globally. Different countries are trying to address the gap through multiple skilling initiatives and frameworks, however, there are 3 big challenges that still exist in digital literacy:

- Multiple digital literacy definitions/ frameworks exist, leading to duplication of effort, thereby creating inefficiency
  - Non-standardised definitions make it challenging to compare and measure levels of digital literacy across countries
  - Duplication of effort through multiple digital literacy frameworks is costly and time-consuming.
- Quality of digital education varies across countries, hampering the cross-pollination of talent and leading to high cost of re-education
  - Cross border movement of people will increase, projected to ~350Mn migrants in 2030, with a majority residing in G20 countries
  - No global standard of digital literacy means a high cost of re-education
  - Standard quality increases portability and employability across global organisations.
- Limited concerted effort to enable the development of digital skills for vulnerable groups, leading to multiple groups lagging behind
  - As per a UNESCO study[43] of 30+ frameworks in 20+ countries, existing digital competence frameworks do not prioritise access and inclusion, resulting in high disparity in digital skills amongst women, senior citizens, and children with disabilities
  - Vulnerable groups like children with disabilities lack basic foundational skills and are hence getting left behind.

Different countries have created different definitions and frameworks of digital literacy to address the growing skill gap for digital skills. There are 30+ global, national, and sub-national frameworks[44] that define different levels of proficiency across disparate competencies including enterprise frameworks such as the International Computer Drivers License (ICDL), Certiport IC3 Digital Literacy Certification Global Standard 5, Microsoft Digital Literacy Standard Curriculum 4, national frameworks such as British Columbia Digital Literacy Framework, Australia's Foundation Skills for Your Future Digital Framework, India's Pradhan Mantri Gramin Digital

39 BCG X Telkom, Powering up a post-pandemic rebound for MSMEs through digital transformation, 2022, https://web-assets.bcg.com/43/67/ a085a86945b2b9fa81a9ae8e0e63/bcg-x-telkom-powerin-gup-a-post-pandemic-rebound-for-msmes-through-digital-transformation-31-aug-2022.pdf

40 World Economic Forum, Future of Jobs, 2020

41 RAND Europe, The global digital skills gap: Current trends and future directions, 2021

42 PwC, Global Workforce Hopes and Fears Survey of 52,195 workers across 44 countries and territories, 2022

43 UNESCO-UNEVOC, How do digital competence frameworks address the digital divide?,

44 UNESCO-UNEVOC, Database 2022, https://unevoc.unesco.org/home/Digital+Competence+Frameworks

Saksharta Abhiyan (PMGDISHA – a rural digital literacy program), etc., and global frameworks such as European Commission's Digital Competence Framework for Citizens (DigComp), UNESCO's Digital Literacy Global Framework, UNESCO's Digital Kids Asia-Pacific framework, the DQ Institute Framework for Digital Intelligence, etc.

However, there is limited harmonisation and consistency amongst them at a global scale. Moreover, there is scope of enhancement in terms of global relevance to address the needs of the population in developing countries and application of the existing frameworks in terms of curriculum, assessment, and measurement of digital literacy levels.

Given that different countries have adopted multiple frameworks, it is difficult to monitor and compare digital literacy levels at a global level. There is lack of available data on the usage of these frameworks. Additionally, it is time-consuming and costly for countries to create and implement new digital literacy frameworks, thereby creating inefficiency. For instance, the estimated time and effort spent on framework design, methodology mapping, feedback solicitation, updates, etc., is upwards of 2 years[45]. Hence, standardisation will lead to efficiency and make it easier for countries to measure and compare digital literacy levels.

Many country-specific qualifications are not recognised globally. This creates a problem for students and workers as their international mobility gets adversely affected and they have to undergo additional courses to acquire qualifications that are recognised in the host country.

Migrants continue to rise globally with a majority (~64%) of migrants residing across G20 countries. ~87% of these migrants fall in the working age group (25-54 yrs)[46]. In 2020, more than 40%[47] of the migrants worldwide were born in Asia, with ~20% coming primarily from 6 countries – India (the largest), China, Bangladesh, Pakistan, Philippines, and Afghanistan. Mexico was the second largest country of origin. As migrants increase from ~280 million to expected ~350 million[48] (4% of the world's population) by 2030, there are associated costs that will hamper their portability and employability. An example of such costs is language proficiency tests. In 2019, the estimated cost of these tests was ~USD 1 billion[49]. Apart from this, there are additional educational costs of migration such as credential evaluation, re-certification through formal/ informal online courses, etc. Therefore, standardisation will lead to easier portability and interoperability of talent across countries.

Digital divide and social inequalities affect opportunities to develop digital skills, especially for vulnerable groups such as children with disabilities, women, rural population, low-skilled workers, and senior citizens. Globally, it is estimated that 40-160 million women may need to change their occupation by 2030 due to automation[50]. According to a UNESCO report[51], women and girls are 25% less likely than men to know how to leverage digital technology for basic purposes, 4 times less likely to know how to program computers, and 13 times less likely to file for a technology patent. Europe's Digital Economy and Society Index (DESI) shows[52] that in 2020, 82% of 16–24-year-olds had at least basic levels of digital skills compared with 35% of 55–74-year-olds having similar skills. Children with disabilities are 42% less likely to have foundational reading and numeracy skills as compared to children without disabilities[53]. Consequently, these children also suffer from a lack of digital skills. Current frameworks do not sufficiently address the digital needs of these vulnerable groups. As a result, they are getting left behind.

45 BCG analysis of existing frameworks such as DigComp, DLGF & DQ Framework
46 Migration data portal, UN Department of Economic and Social Affairs 2020
47 World Migration Report 2022, link: https://worldmigrationreport.iom.int/wmr-2022-interactive/
48 World Economic Forum
49 Calculated by multiplying number of international student flow across G20 (~4.2 mn) and average cost of re-education per person (~USD 220); This cost includes cost of language proficiency tests such as TOEFL, IELTS etc. which are accepted in 4 countries for work purposes, 100+ countries for study purposes. Avg price of IELTS is taken as ~USD 250 and TOEFL, as ~USD 190
50 McKinsey, The Future of Women at Work: Transitions in the Age of Automation, 2019
51 UNESCO, I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education. UNESCO Equals Skills Coalition, 2019, https://unesdoc.unesco.org/ark:/48223/ pf0000367416.page=1
52 European Commission, Digital Economy and Society Index (DESI) 2020: Human Capital, 2020, https://digital-strategy.ec.europa.eu-/en/policies/ desi-human-capital
53 UNICEF, Geneva Global Hub for Education in Emergencies,2022, https://eiehub.org/education-in-emergencies-and-disability-inclusive-education#:~:text=Compared%20to%20children%20without%20disabilities,to%20have%20never%20attended%20school.

Despite existing frameworks and initiatives, it is increasingly being observed that even students with tertiary education are unable to meet the level of digital skills required by employers. For example, the UK's Learning and Work Institute[54] found that 52% of employers thought that young people were not graduating from full-time education with sufficiently advanced digital skills. The reasons behind this include lack of digitally relevant content in the curricula, lack of awareness among institutions regarding digital skills required by employers, and poor teaching training methods.

To address the issues faced in digital literacy and skills effectively, the B20 Digital Transformation Task Force would like to draw attention to the following policy action:

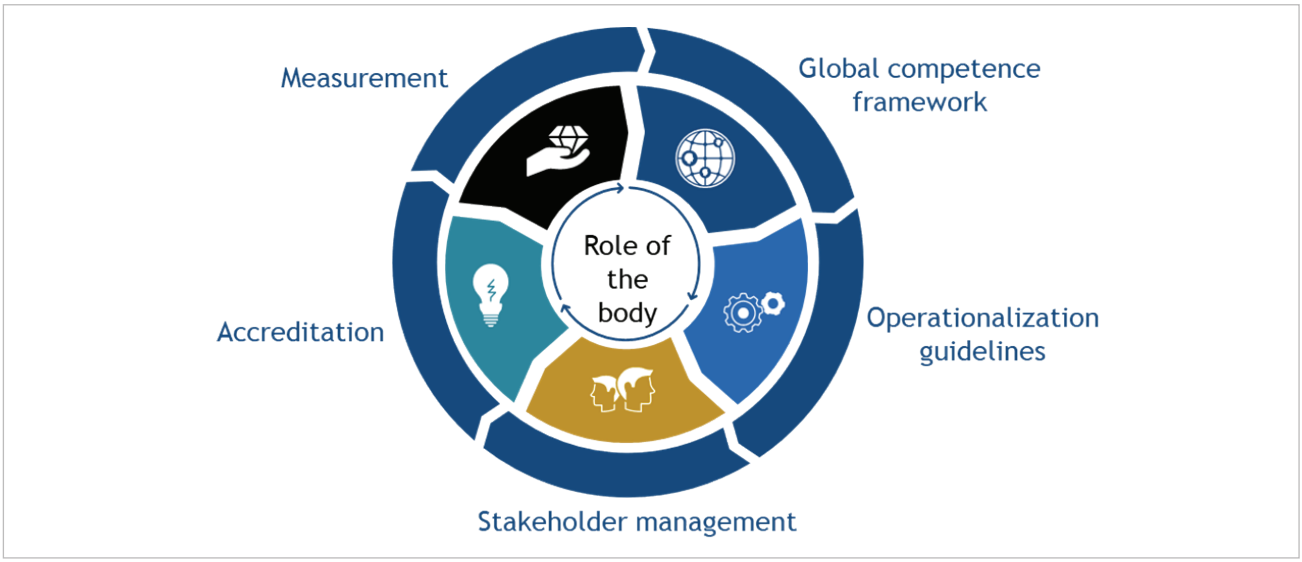
Policy Action 2.1: Institutionalise a global body to achieve the mandate of setting unified standards & metrics for digital literacy, adopting a global competence framework, sharing best practices, accrediting institutions and teachers trained under the framework, and operationalising the guidelines for developing learning material, curriculums, and assessments through multi-stakeholder and cross-national partnerships

In this context, we have established that there are multiple frameworks and definitions of digital literacy which aim to address the needs of digital literacy in education, however, there is no global standard that exists. It is important that G20 countries adopt a single global standard definition and framework for digital literacy.

We believe that this will enable cross-country comparison of digital literacy levels, which will in turn lead to focused reforms, the sharing of best practices, and tracking progress on a global scale. Thereby, we recommend the following:

Establish a global body for establishing digital literacy standards to enable international portability, the creation of an inclusive and ready workforce of the future, and global measurement and comparison of digital literacy levels

Exhibit 7: Framework of the global body



54 Learning and Work Institute, Disconnected, Exploring the Digital Skills Gap, 2021 https://learningandwork.org.uk/resources/research-and-reports/disconnected-exploring-thedigital-skills-gap/

Mission

Ensure social inclusion, reduced digital disparity, and enhanced digital empowerment and access for citizens across the world

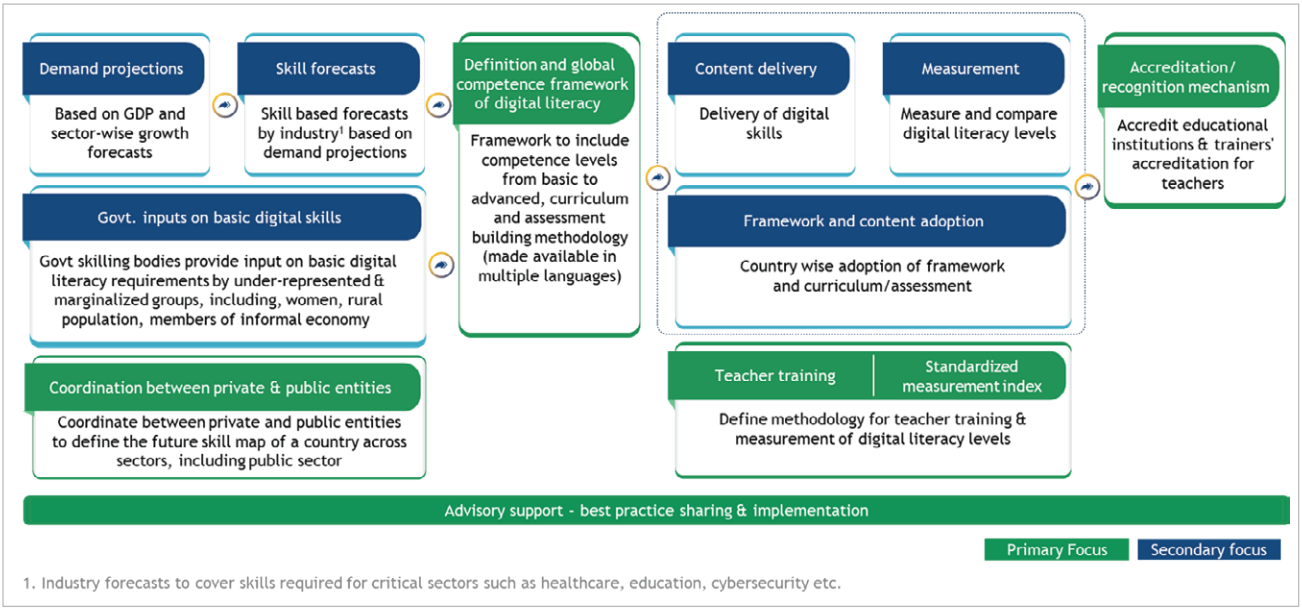
Objective

- Enable the creation of an inclusive and ready workforce of the future, with focus on developing digital skills for the most vulnerable groups
- Enable international portability and interoperability of talent
- Allow countries to measure and compare digital literacy levels

Role of the body

- **Measurement:** Define a standard measurement index to monitor and compare digital literacy levels
- **Global competence framework:** Adopt a definition and global competence framework relevant to a broader range of development contexts and enable international portability by setting-up minimum levels for the acquisition of competencies
- **Operationalisation guidelines:** Provide practical guidelines to develop learning material, curriculum and assessments, promote the widespread application of digital equipment in teaching methods, and incorporate experiential learning into traditional modes of education; share global best practices for the benefit of members
- **Stakeholder management:** Engage in multi-stakeholder partnerships, such as with educational institutions and national skilling programs for wider acceptance and efficient adoption
- **Accreditation:** Recognise institutions and teachers trained under the adopted digital literacy framework

Exhibit 8: Primary & secondary focus of the body in the literacy value chain



The body will behave as a nodal agency between the industry, the Government, and educational institutions. It will collect inputs from the private and public sectors on future digital skills required by both. This skill map will be based on demand projections across sectors. Industry forecast should cover skills required for critical sectors such as education, healthcare, cybersecurity, etc. For example, in the healthcare sector, there is a need for systematic approach to digital skilling for all categories/cadres of health workers including doctors, medical students, nursing, midwifery, and allied health workers to make them future-ready. This can be done by integrating digital skilling as a core content of medical education and continuing professional development.

Moreover, it will coordinate with government skilling bodies for inputs on digital literacy skills required by vulnerable groups including women, rural population, members of the informal economy, etc. Based on the inputs received, it will develop a global competence framework of digital literacy, with levels ranging from basic and intermediate to advanced. It will also develop guidelines for curriculum and assessment building methodology (e.g., digital topics to be included in school and university curriculums, skills to be tested for industry readiness of students, etc.).

Countries can voluntarily adopt the new framework and upgrade curriculum and assessments based on it. The body will not interfere with local content delivery and adoption. Rather, it will work with national governments and school and university boards to enable implementation. Further, it will also share global best practices for learning and enablement.

It is recognised that augmenting teachers' capability to use technology as a learning enabler and updating their digital skills is equally important. Hence, the body will also develop a methodology for training teachers under the new framework, which educational institutions can implement directly. For any support required, the body's advisory arm will actively work with the respective entity.

The last leg of the value chain is the measurement of change in digital literacy levels and accreditation. The body will define a standardised index based on the framework and methodology for its calculation. Countries can independently collect the required data and report index numbers. The body will also devise an accreditation mechanism for educational institutions as well as teachers to recognise a standard of digital skills in the market.

Detailed description

- **Measurement:** The body should define a standardised measurement index to enable the measurement and comparison of digital literacy levels, thereby helping countries devise interventions targeted towards areas with acute needs. Countries can implement changes in education plans and establish action areas to improve digital literacy levels in schools, based on measurement outcomes.
- **Framework & Definition:** B20 Indonesia recommended the establishment of a digital competency map as well as a common digital skills taxonomy. The objective was to map the current levels of digital competence across countries and industries. We call on the G20 to build on this effort and other existing initiatives at an international level such as the World Economic Forum Global Taxonomy and UNESCO's Digital Literacy Global Framework, through this body.

  Digital literacy is a multi-dimensional concept. Though there are multiple definitions followed by countries, there is no universally accepted definition. However, focusing solely on technical aspects of digital literacy, such as using tools, can exclude important aspects such as awareness of cognitive and ethical concerns of digital technologies . Cognitively, a user can process, critique, and synthesise multiple sources of information. Ethically, knowing how to discern between what is an appropriate use of technology and media is important. Hence, the body needs to establish a broader and holistic definition that can subsequently be universally implemented.

  This definition should be anchored around a global competence framework which can be a modified version of existing global frameworks with global relevance and context, to avoid investing time and effort into devising an entirely new framework.
- **Operationalisation of the framework:** The body should aim to build effective lifelong learning systems by improving existing curricula to include digital topics, promoting the widespread application of digital equipment in teaching methods and utilising modern teaching techniques, and incorporating experiential learning into traditional modes of education.

  Many education systems are not equipped to teach children digital skills as they lack proper infrastructure, equipment, training, curriculum, or learning benchmarks. This gap is more pronounced in developing countries.

It should aim to amend existing curricula to fit the needs of a changing digital landscape apart from the development of basic ICT and digital competencies (e.g., computer and coding skills should be complemented by learnings around digital entrepreneurship, daily use-cases of emerging technologies like AI and IoT, etc.,). This can be done through cooperation between educational institutions and private players to ensure that curricula reforms are aligned with future business needs and innovations.

Research shows that students who learn through experiential learning techniques, for example by doing experiments and hands-on training, understand more and perform better on tests. There are two ways to implement this:

- By incorporating an apprenticeship model of learning where students get the flexibility to learn skills through real-world experience and practical examples
- By incorporating immersive technologies like visual and mixed reality virtualised learning environments and labs and AI-enabled learning models that create a safe and controlled environment for students to learn

The body will share best practices and work with individual member countries to enable the adoption of the defined framework, update curricula and assessments, and include digital technologies in the learning environment.

- **Stakeholder management:** This global body will not replace, rather interface and synchronise efforts with existing bodies/ frameworks, to maintain a global literacy standard. The partnership model, can include, but is not limited to:

Strategic partners

- Partner with governments, international organisations, and national skilling bodies to address the digital literacy requirements of vulnerable groups, share best practices, and measure digital literacy levels
- Partner with bodies with existing global frameworks to synchronise and adopt a global framework which is inclusive and relevant to many developmental contexts.

Community members

- Partner with industry associations to build skill forecasts and incorporate it in the global framework
- Partner with academic institutions and educational boards to foster the adoption of the framework into educational curriculums and further provide recognition / accreditation.

Commercial partners

- Establish a global network of training partners who can provide implementation support and advisory to institutions on how to adopt the framework, train teachers, develop curriculum, and run assessments.

Recommendation 3

Promote enterprise transformation for MSMEs through access to sustainable finance, a globally recognised, sector-specific digital toolkit, and a favourable regulatory environment

Policy actions

3.1 Expand efforts to provide sustainable financing to MSMEs for adopting digital technologies and complimentary services

3.2 Establish a globally recognised digital toolkit and framework, supported by a favourable regulatory environment, that enables the creation of a digital ecosystem and provides end-to-end support to MSMEs in their digital transformation journey with a focus on creating a user-friendly and accessible platform that caters to the needs of MSMEs of different sizes and industries

Leading Monitoring KPI	**Owner: G20 Countries**	
MSME digital maturity (based on MSMEs using some form of ERP or CRM)[56]	Baseline **31%** (2021)	Target **35%** (2025)

Source: OECD & Eurostat Database

56 Calculated using 2 indicators – "% businesses using ERP or CRM software", captured under ICT Access and Usage by Businesses database, a selection of 51 indicators, based on the 2nd revision of the OECD Model Survey on ICT Access and Usage by Businesses. From OECD & Eurostat database, May 2023, https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS#

Recommendation 3 contributes to the achievement of UN's SDG 5: gender equality; SDG 8: decent work and economic growth; SDG 9: industry innovation and infrastructure; and SDG 10: reduced inequalities

Policy action 3.1 contributes to target 9.3 "Increase the access of small-scale industrial and other enterprises, in particular in developing countries, to financial services", given the recommendation's focus on sustainable financing, and target 9.2 "Promote inclusive and sustainable industrialisation" given the relevance for the potential of MSMEs to drive economic growth. There is also significant overlap with targets from SDG 8 – target 8.3 "Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalisation and growth of micro-, small- and medium-sized enterprises, including through access to financial services" and target 8.10 "Strengthen the capacity of domestic financial institutions to encourage and expand access to banking, insurance and financial services for all."

The expected benefits of financing and digitising MSMEs also support SDG 10 and 5 generally, given that a significant number of MSMEs are run by women entrepreneurs and also comprise a key pillar of developing economies. Thus, policy action 3.1 supports target 10.1 (income growth of the bottom 40% of the population), target 10.2 (promote the social, economic and political inclusion of all), and target 5.5 (women's participation in political, economic and public life) by enabling MSMEs to succeed via sustainable financing.

Policy Action 3.2 contributes to SDG target 5.5 and target 10.1 "By 2030, progressively achieve and sustain income growth of the bottom 40 per cent of the population at a rate higher than the national average." Additionally, the policy action ties into 9.b "Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities".

CONTEXT

MSMEs are the backbone of the global economy, accounting for over 90% of global businesses and half of global employment[57]. MSMEs represent a very critical pillar for GDP growth and economic activity. In emerging economies, estimates show that MSMEs are the source of over 70% jobs and half of national GDP[58], with formal MSMEs contributing up to 40% of national GDP and informal MSMEs yielding even more substantial economic impact[59]. To put this in context, India is home to more than 63 million MSMEs, a majority of which are in the micro-enterprise category[60]. MSMEs form a key pillar of the Indian economy, accounting for over 30% of the GDP, 45% of manufacturing output, and providing employment to approximately 111 million people[61]. Women own about one-third of micro and small enterprises and one-fifth of medium-size enterprises in emerging countries[62]. Women-owned enterprises are more likely to be informal than male-owned enterprises.

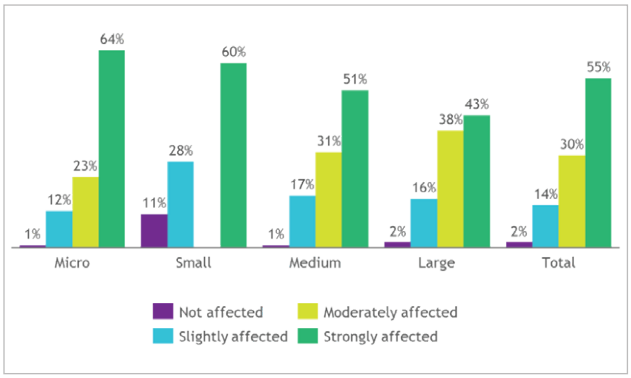
MSMEs enable communities and other businesses around them through forward and backward linkages in the economy and will continue

57 World Bank, Small and Medium Enterprises (SMEs) Finance
58 World Bank; Organization for Economic Cooperation and Development
59 BCG X Telkom, Powering up a post-pandemic rebound for MSMEs through Digital Transformation, August 2022
60 ICRIER, MSMEs Go Digital (based on survey conducted during the 2nd COVID wave), 2020
61 Annual report, Ministry of Micro, Small & Medium Enterprises, 2021-22, https://www.pib.gov.in/PressReleasePage.aspx-?PRID=1744032
62 AFI, SME Finance Working Group, Survey Report on Alternative Finance for MSMEs, 2020

to play a major role in ensuring economic opportunity in coming years. In this decade alone, they are expected to account for approximately 420 million new jobs globally[63].

COVID-19 impacted all businesses, regardless of scale, but MSMEs were hit particularly hard. According to a UNCTAD[64] survey of businesses in over 100 countries, the vast majority were strongly affected by COVID-19. The disruption was especially hard for micro-enterprises where over 64% were impacted as compared to small (60%), medium (51%), and large companies (43%)[65]. Women-led enterprises were hit harder than men-led ones - 64% of women-run enterprises claimed to be "strongly affected" by the crisis as compared to 52% of men-run or owned firms[66].

Exhibit 9: Impact on MSMEs during pandemic



Source: International Trade Centre calculations based on ITC COVID-19 businesses impact survey,

Data collected 21 April- 2 June 2020

Note: Respondents were asked 'How have your business operations been affected by COVID-19' and 'How many full-time employees does the business have?'

Definitions: Microenterprises up to 4 employees; small firms, 5-19 employees; medium sized firms, 20-99 employees and large firms, 100 or more employees. Data on 2170 businesses in 121 countries. Response rates vary across countries and regions

Pre-pandemic, less than 50%[67] MSMEs indicated large online payments from clients or to suppliers. While relatively few businesses had a dedicated website to sell their products or services. Evidence from business surveys worldwide suggests that up to 70% of Small- and Medium-sized Enterprises (SMEs) increased their use of digital technologies due to COVID-19[68]. Those who failed to adopt digital, faced disproportionate challenges in their efforts to stay competitive. Embracing digitalisation can make MSMEs more resilient and competitive, as well as facilitate better access to international markets.

A survey[69] of MSME owners across select developing countries indicated that MSMEs had started using low-barrier digital tools (e.g., instant messaging or social media for communication and connecting with consumers) during the pandemic, whereas high-barrier digital adoption (e.g., ERP systems) was less common, especially among women.

Evidence[70] shows that factors that constrain MSME digital transformation are high implementation cost (56%), a lack of a digitally skilled workforce (40%), the uncertain economic environment (35%), low awareness of government support (30%), and not having the right technology partners (28%). The challenges[71] that MSMEs face in digital adoption can be summarised as follows:

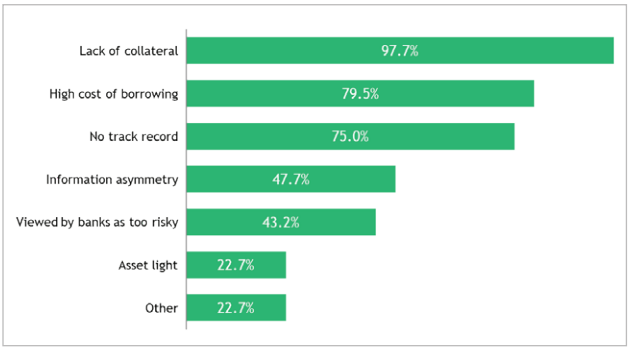
- **Access to finance:** This is the biggest challenge, whether for working capital to scale business or as investment capital for the adoption of digital technologies
- **People and capabilities:** How to attract and retain the right talent with digital capabilities
- **Business strategy and return on investment:** How to measure and guarantee return on investments on technology and associated initiatives

63 United Nations, MSMEs: Key to an inclusive and sustainable recovery, 2021
64 UNCTAD, The COVID-19 Pandemic Impact on Micro, Small And Medium-Sized Enterprises, Market Access Challenges And Competition Policy, Geneva, 2022
65 International Trade Centre, COVID-19: The Great Lockdown and its Impact on Small Business, July 2020
66 International Trade Centre, COVID-19: The Great Lockdown and its Impact on Small Business, July 2020
67 OECD, G20/OECD-INFE report Navigating the storm: MSMEs' financial and digital competencies in COVID-19 times, 2021, www.oecd.org/finance/navigating-the-storm-MSMEs-financial-and digitalcompetencies-in-COVID-19-times.htm
68 OECD, The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship, OECD Publishing, 2021, Paris, https://doi.org/10.1787/bdb9256a-en.
69 Centre for Financial Inclusion, Digital Adoption of MSMEs During COVID-19, Sep 2022
70 Microsoft Singapore and the Association of Small & Medium Enterprises, 2020 SME Digital Transformation Study, October 2020
71 World Economic Forum, COVID-19 and Technology Adoption in Small and Medium-Sized Enterprises: The Impact and the Way Forward White Paper, December 2021

- **Infrastructure and processes:** How to identify the right use cases and define a roadmap to implement them while keeping pace with new technological developments
- **Technology readiness:** How to experiment with technology cheaply and quickly and access and share experiences about success, failures, and best practices
- **Ecosystem maturity:** How to define a strategy around the entire value chain and collaborate with other players to solve for common problems

The International Finance Corporation estimates[72] that 65 million firms (or 40% of formal MSMEs) in developing countries have an unmet financing need of USD 5.2 trillion every year, which is equal to 1.4 times the current level of global MSME lending. In addition, there is USD 2.9 trillion potential demand from informal enterprises. The gap volume varies from country to country. East Asia and the Pacific account for the largest share (46%) of the total global finance gap[73], followed by Latin America and the Caribbean (23%), and Europe and Central Asia (15%). The majority of the women-owned MSME finance gap is in the low-income and lower-middle-income countries, where it represents more than 50% of the total finance gap, on average[74].The challenges faced by MSMEs in accessing traditional finance are highlighted in Exhibit 10 below.

Exhibit 10: Challenges faced by MSMEs in getting funding, %



Source: AFI Alternative SME Finance

The figures reflect the % of the respondents who identified the challenge as being present in their jurisdiction. Multiple responses were possible

In order to address these challenges, it is important to have a holistic policy around enabling a digital ecosystem for MSMEs. In an effort to guide G20 towards enabling digital transformation of MSMEs, the B20 Digital Transformation Task Force seeks to draw their attention towards two policy actions:

- **Policy action 3.1:** Expand efforts to provide sustainable financing to MSMEs for adopting digital technologies and complementary services
- **Policy action 3.2:** Establish a globally recognised digital toolkit and framework, supported by a favourable regulatory environment, that enables the creation of a digital ecosystem and provides end-to-end support to MSMEs in their digital transformation journey with a focus on creating a user-friendly and accessible platform that caters to the needs of MSMEs of different sizes and industries

Policy Action 3.1: Expand efforts to provide sustainable financing to MSMEs for adopting digital technologies and complementary services

MSMEs face several issues with respect to access to finance. The barriers to MSME finance exist from both supply and demand side. From the supply side, barriers include information asymmetry due to inadequate credit registries and credit scoring and lack of awareness and understanding of the financial system[75]. Further, the underwriting systems of lenders continue to evolve at a slower pace than required. From the demand side, barriers include a lack of adequate collateral (partly due to banks' limited appetite towards interest caps and high-risk assets of MSMEs), lack of proper accounts, managerial skill deficiencies, financial literacy, and lack of formalisation of MSMEs.

In order to tackle these barriers, governments should identify the core problems and review policies toward promoting inclusive finance.

72 World Bank
73 The difference between the estimated demand or access to finance and the extent to which this demand has been met is termed as the MSME finance gap.
74 AFI, SME Finance Working Group, Survey Report on Alternative Finance for MSMEs, Dec 2020
75 ADB (202) Asia Small and Medium-sized Enterprise Monitor 2020 Volume I: Country and Regional Reviews. Manila: http://dx.-doi.org/10.22617/TCS200290-2.

Mechanisms to access traditional finance need to be simplified and options to access alternative finance need to be made available. Unless MSMEs get access to capital, they will be limited in their endeavours to achieve enterprise-wide digital transformation.

1. G20 countries should strengthen access to traditional debt-based bank financing

Increased access to capital will enable MSMEs to invest in transforming their own ways of working. The Primary source of formal capital for MSMEs is bank lending. Governments should identify the core issues faced by MSMEs in accessing bank credit and consider innovative ways and new technologies to enhance credit access as well as improve their customer experience. Measures may include allowing flexible collateral options beyond fixed assets, such as intellectual property and accounts receivable, improving credit guarantees, and other risk diversification instruments and underwriting methodologies. Methods for credit assessment that allow credit line extension to meet their changing working capital needs should be evaluated. Alternative approaches to credit screening should be explored.

2. G20 countries should enhance MSME access to diverse non-traditional financing instruments and channels through a clear and comprehensive regulatory framework and outreach program

Alternative credit sources have largely complemented traditional credit methods. Microfinance institutions and Non-Banking Financing Companies (NBFCs) are also bridging the credit flow gap to MSMEs. For example, in India, NBFCs have developed nuanced credit assessment techniques to better judge the creditworthiness of MSMEs, which ensures an easier loan process and faster turnaround time. This incentivises MSMEs to apply to formal channels for credit.

In addition, financial inclusion has gained pace in part due to the advent of financial innovation and emerging technologies. A recent survey of 79 countries suggests that the total market volume of credit by FinTech and BigTech companies in 2019 was about ~USD 800 billion globally, with China, the USA, and the UK being the largest markets for FinTech and Asia being the largest market for BigTech[76]. Digital lending has increased drastically in India with the advent of marketplace lending platforms in addition to balance sheet lending. Digital finance is projected to increase global GDP in emerging economies by up to 6% (about USD 3.7 trillion) by 2025[77].

Digitalisation is helping MSMEs resolve multiple challenges and barriers as it provides cost and time advantage over traditional methods. For example, digital loan fulfilment has 30-40% cost advantage over traditional methods, which are predominantly paper-based processes, and 40-50% for cost of underwriting operations and servicing[78].

Many SMEs face a challenge in maintaining working capital to run their businesses. Loan processing via traditional banks has many pain points such as long processing time, lack of transparency in timelines, and insufficient loan sizes[79]. Digital lending and payment platforms solve these challenges in 3 ways: faster loan approval, credit underwriting insight, and operating cost efficiency while ensuring consumer protection and financial stability. The Indian government's concerted effort towards the development of digital payments through Unified Payments Interface (UPI) as part of the "India Stack" initiative, has increased the level of financial inclusion to over 90%[80], which is further increasing with new innovations to UPI, allowing for offline transactions by Indian nationals and merchant transactions by foreign nationals / non-resident Indians (NRIs) coming from G20 countries. According to Omidyar-BCG research, MSME digital lending through UPI has the potential to reach USD 80-100 billion in annual disbursement.

76 Cornelli, Giulio, and others, Fintech and big tech credit: a new database. BIS Working Paper, No.887, 2020, https://www.bis.org/publ/work887.pdf.

77 United Nations Economic and Social Commission for Asia and the Pacific, MSME Access to Finance: The Role of Digital Payments, MSME Financing Series No.7, Bangkok: United Nations, 2022, https://www.unescap.org/kp/2022/msme-financing-series-role-digital-payments

78 Omidyar-BCG research, Credit disrupted: Digital MSME Lending in India, 2019

79 Omidyar-BCG research, Credit disrupted: Digital MSME Lending in India, 2019

80 UNESCAP, MSME Access to Finance: The Role of Digital Payments, 2022; Zetzsche and others, 2020

The increased adoption of contactless and other payment solutions has also been leveraged to disburse government benefits to vulnerable groups in remote areas, during the pandemic. At the same time, disruptions taking place outside of known regulatory parameters have raised concerns about consumer protection, financial stability, and market integrity among advanced and developing countries. The activities of many new entrants, which are outside the regulatory perimeter, are growing rapidly. This may threaten the financial stability of economies due to enhanced connectivity with incumbents and the cross-pollination of systemic risks. There is also a regulation hierarchy according to which tech giants' activities that do not affect core financial systems' stability do not warrant interventions like other financial institutions.

Given this scenario, a regulatory framework will act as a key enabler for the development of alternative finance mechanisms for MSMEs as these instruments carry more risk than traditional finance mechanisms. Countries should do a rigorous and comprehensive risk and regulatory gap analysis to determine the risks associated with new technologies, products, and services and the appropriate and timely regulatory responses, keeping in mind that regulations should be proportionate to the risks of different financing instruments. Governments should establish a regulatory framework that avoids undue administrative burden on MSMEs to apply for credit, ensures transparency and safety, and incentivises MSMEs to maintain good corporate governance. All these elements lower the barriers for change for MSMEs and will help drive the adoption of digital ways of working.

3. G20 countries should engage in active outreach and market engagement through communication portals where information about accessing alternative finance mechanisms is made available

MSME-targeted interventions have only reached businesses operating in the formal sector, precluding firms that operate in the informal sector. The issue is more prominent in emerging and developing economies which house a greater level of informal employment. A substantial share of MSMEs in emerging and developing economies cited "lack of awareness of available measures" as a reason for not obtaining financial support in 2020 including Sub-Saharan Africa (39%); Latin America (35%); South Asia (33%); and the Middle East and North Africa (30%)[81], showing that many governments have seemingly failed to effectively communicate the availability of relief programs for local MSMEs.

Increasing awareness about finance support such as funds, grants, and other non-traditional sources of finance is key to achieving the financial inclusion of MSMEs. Governments should develop effective communication strategies and build portals aimed at identifying channels for application, eligibility criteria, awarding process, and requirements for companies to access specific subsidies or support. Creating awareness of new digital solutions to close the MSME financing gap is critical[82].

Policy Action 3.2: Establish a globally recognised digital toolkit and framework, supported by a favourable regulatory environment, that enables the creation of a digital ecosystem and provides end-to-end support to MSMEs in their digital transformation journey with a focus on creating a user-friendly and accessible platform that caters to the needs of MSMEs of different sizes and industries

Recent research from BCG[83] shows that 7 in 10 digital transformation programs fail to live up to their goals. Problems include a lack of proper implementation, technologies not working as expected, and manual processes continuing in parallel, etc. It is even more challenging for small and micro enterprises that lack the framework and resources to implement a digital transformation program. MSMEs need a sector-specific digital

81 Facebook, World Bank and OECD, Global State of Small Business Report: Reflections on six waves of data collection, December 2020

82 BCG X Telkom, Powering up a post-pandemic rebound for MSMEs through Digital Transformation, August 2022; Tempo, QRIS Limit Raised to Rp10million Starting Today,2022

83 BCG- Flipping the Odds of Digital Transformation Success, 2020; https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation

toolkit that can help them create a roadmap to digital adoption. In addition, it should be complemented by the right regulatory environment, which removes administrative barriers and enables them to expand their digital footprint in both internal ways of working and external relationships and transactions.

1. G20 countries should establish a digital toolkit and framework which comprises, but is not limited to, a digital use-case library, maturity assessment tools, and list of online platforms and digital training tools to provide all the necessary information from hiring and upskilling talent to adopting the right technology for MSMEs and staying safe and secure online

In order to start their digital journey, MSMEs first need to be aware of the potential technology deployments and their value generation. The G20 should establish a sector-specific customisable digital toolkit and framework at first level which countries can build upon, comprising, but not limited to, the following areas:

- **Maturity assessment tools:** Tools to help MSMEs identify gaps and strengths, pinpoint use-cases that need to be prioritised, enabling them to develop a digital investment strategy
- **Use-case[84] catalogue:** Comprising tried-and-tested digital and emerging technology use-cases, providing an overview of business cases, description of technical solutions, KPI quantification, including ROI estimates as well as benefits and challenges of deploying solutions
- **Online platforms:** Share success stories of other MSMEs and provide useful information about funding and support services which solve the information fragmentation among MSMEs. Additionally, create a mechanism for MSMEs to provide feedback on the platform and its contents, and use this feedback to improve the platform. Integrating MSMEs with online platforms might help less-equipped MSMEs from very traditional industries to get exposure to digitalisation
- **Digital skilling tools:** MSMEs, many owned and managed by entrepreneurs, need access to digital literacy courses, ideally tailored to the local market and their needs. Having the right digital talent is instrumental in realising ROI for digital investments. The toolkit should provide skilling tools to upskill the existing workforce as well as hire the right people to implement a digital transformation program. Local business associations and chambers of commerce may be appropriate training partners in this case. Additionally, create a mechanism for MSMEs to share their training needs and challenges, and use this feedback to improve the digital training tools and their contents

B20 use case library made by the digitalisation task force under B20 Italy team and further improved by the B20 Indonesia team can be used as a starting point for the tool kit. It can be further complemented by adding use-cases in emerging businesses.

One of the major barriers to digital adoption among MSMEs pertains to a dearth of relevant knowledge pertaining to the operational and beneficial aspects of digital tools. A Brazilian national survey[85] on the adoption of digital tools by industrial companies showed that a lack of technical knowledge about digital technologies was the main internal barrier after the high implementation costs for MSMEs in a list of eight possible barriers. On the other hand, it was only the fifth main barrier for large companies.

To stimulate the uptake of digital tools by MSMEs, it is imperative to create awareness regarding the digital technologies and toolkit. G20 countries should initiate campaigns aimed at promoting the offerings and benefits of digital technologies and the toolkit. An online help centre and consultation via the portal could be established to cater to specific queries like application of tools, costs, return on investment, etc.

A good example of this intervention would be the Mittelstand 4.0 Competence Centres[86], implemented by the Federal Ministry for Economic Affairs and Energy in Germany.

84 A use case is a description of a generic, reusable practice or procedure, usually described in the form of a scenario that represents typical business operations, related or unrelated to a specific industry sector.

85 Brazilian National Industry Confederation, Special Survey 83: Industry 4.0 Five years later, April 2022. https://www.portaldaindustria.com.br/statistics/special-survey-industry-4-0/ .

86 Federal Ministry for Economic Affairs and Energy, Mittelstand-Digital: Strategies for the Digital Transformation of Business Processes, March 2017

The Centres act as nodes for regional consolidation of information and competence-matching to support MSMEs in digital adoption. They help SMEs gauge their current stage of digitisation, support the development of a bespoke digital roadmap, and pinpoint technical solutions that are economically viable for their context. In addition, they also carry out several activities such as training courses, webinars, events, roadshows, workshops, and expert meetings.

The digital toolkit could also be implemented in a phygital manner wherein resources, training material, information portal, etc., and other tools are made available digitally and local ministries initiate physical drives and campaigns to help MSMEs use the tools.

There are existing resources and technology solutions made available by governments and businesses to help digitise MSMEs. This toolkit can act as an aggregator and promoter of available content for G20 countries, to avoid duplication of services already produced by companies.

2. The G20 should promote public and private investment towards digital solutions and platforms catering to the needs of MSMEs and create awareness about the use of digital technologies to enable easier adoption of digital

Most of the world is working to digitalise, a trend that has accelerated over the course of the pandemic, and SMEs are at the risk of being left behind. A survey of businesses in Singapore revealed that only 50% SMEs had plans for digital transformation, compared to over 98% of larger companies[87]. This is majorly because digital solutions are often designed for large enterprises and are difficult to scale down for SMEs. The G20 should promote public-private investment towards digital solutions and platforms that are customised to the needs of MSMEs to foster digital adoption.

3. G20 countries should promote favourable regulatory environment and e-government services to alleviate the administrative burden and enable greater market access for MSMEs

Several studies show that MSMEs struggle to expand outside their home markets. Unlike large companies, many SMEs do not have the resources to conduct market research to expand into new markets and are hence restricted to following domestic opportunities and growing marginally. In the EU, nearly all of 20% of small businesses with e-commerce sales sell within their own economy. Only 4% of the overall market sells outside the EU. A similar trend is observed in other countries as well[88].

Additionally, in countries where MSMEs want to run their business digitally, they encounter regulatory hurdles which create impediments to doing so. In order to alleviate these problems, G20 countries should focus on policy interventions at two levels:

3a. Enable MSMEs to operate without administrative burden through supportive regulatory and business infrastructure

An important factor for MSMEs to thrive in a digital economy is to have supportive legal, regulatory and business infrastructure. Firstly, have laws that support digitalisation uptake. For example, the existence of laws on digital signature, electronic authentication, etc. The main objective is to ensure that online contracts, transactions, and approvals can be done quickly and seamlessly. Governments can utilise international instruments such as model law on e-sign developed by United Nations Commission on International Trade Law (UNCITRAL)[89] as guidance to develop local laws.

Secondly, MSMEs often have to deal with complex administrative systems. Governments should focus on creating one-stop shops and digital portals (e.g., certification assistance, tax administration and compliance portals etc.) where MSMEs can find all the information on how to deal with administrative and legal requirements that facilitates a conducive business environment.

Governments should also promote the adoption of digital ecosystems that are able to automate the verification of regulatory obligations and compliances with international standards.

A good example of this would be the unified system of permits launched by the government of Chile[90] in 2019. It is an online platform intended to

87 Centre for Financial Inclusion, Digital Adoption of MSMEs During COVID-19, Sep 2022

88 OECD, "SMEs in the online platform economy," in the digital transformation of SMEs, February 2021.

89 UNCITRAL, Guide to the Enactment of UNCITRAL Model Law on Electronic Signatures, 2001

90 Chile - Launches new platform for online processing of permits for investment projects I Investment Policy Monitor I UNCTAD Investment Policy Hub, 2019

simplify and speed up the process of obtaining permits for investment projects. The platform has created a single window system, bringing together 182+ license and permit procedures, previously spread across 29 different public institutions. The new system allows users to access all required documentation, start online procedures, check the status of the application, and receive online updates on its progress, all under one single online platform.

3b. Facilitate access to digital platforms and systems to promote higher market access to MSMEs

Governments can help MSMEs to connect with consumers and other businesses through e-commerce platforms. This enables greater market access to MSMEs. Each country should have such platforms which are best suited for respective country's requirement. For example, India has launched Open Network for Digital Commerce (ONDC) platform to help local businesses sell directly to consumers using e-commerce without charging any transaction fees.

Further, there are many complex procedures involved in international trade, which can be a burden for MSMEs with limited resources. Exporters are required to submit documentation such as certificates regarding safety and security, evidence of payments, and customs declaration, among other requirements, to trade authorities. According to WTO, this complexity increases trade costs, particularly in developing countries[91]. Digitalisation can help solve this problem. Governments should promote electronic methods of submitting documents from existing digital repositories and managing financial transactions. These will facilitate transparency in trade and simplify compliance for MSMEs.

An example of enabling MSMEs to trade globally through digitisation is the UK's Digital Exporting Programme established by its Department of International Trade[92]. It has set up tools such as selling online overseas (SOO) tool to help MSMEs find right marketplaces to list products, understand seller requirements, and take advantage of special deals. Further, it aids sellers in getting market intelligence, finding events/trade fairs to participate in and receive one-to-one support tailored to specific MSME needs.

91 Maria Vasquez Callo-Mùller, Micro, Small And Medium Enterprises (MSMEs) And The Digital Economy, 2020

92 Government of UK, Selling online overseas with the Digital Exporting Programme 2014

Recommendation 4

Promote digital trust by developing harmonised cybersecurity standards and frameworks and bridging cybersecurity skill gap while fostering greater multilateral cooperation around cyber space and enabling wider trust around digital systems and processes

Policy actions

4.1 Institutionalise a global body with mandate of harmonising and advocating cybersecurity standards and bringing in a greater degree of multilateral cooperation for shared goals of cyber action

4.2 Improve the trustworthiness of digital ecosystem and work towards a cyber-inclusive future by advocating cyber-awareness till the grassroots level

4.3 Bridge the cybersecurity skill gap by facilitating faster development of cyber talent pipeline through increased investment in existing cyber-skilling institutes, complemented by building National Cyber Academies, through the public-private partnership route

Leading Monitoring KPI	Owner: G20 Countries	
Minimum score achieved by a G20 country on Global Cybersecurity Index[93] (composite of 20 indicators)	Baseline **50** (2021)	Target **90** (2025)

Source: ITU

93 Global Cybersecurity index (launched in 2015 by ITU) measures each country's level of development and areas of improvement along five pillars – (i) Legal Measures e.g., some form of cybersecurity regulation, (ii) Technical Measures e.g., Active CIRTs, (iii) Organizational Measures e.g., National Cybersecurity Strategies, (iv) Capacity Development e.g., Cyber-awareness initiatives, and (v) Cooperation e.g., cybersecurity public-private partnerships and then aggregates it into an overall score.

Recommendation 4: contributes to the achievement of UN's SDG 4: quality education; SDG 9: industry innovation and infrastructure; and SDG 17: partnership for the goals

This recommendation supports targets from SDG 9 focused on (digital) infrastructure development, given that a global body for cybersecurity standards would support tech innovation and cooperation. Target 17.8 is directly relevant as it refers to full technology operationalisation and worldwide implementation.

It ultimately enhances the global industrial network in line with target 9.2 by setting harmonised global standards for technology and developing more efficient interoperability mechanisms. Moreover, it contributes to the achievement of target 17.16 "Enhance the Global Partnership for Sustainable Development, complemented by multi-stakeholder partnerships that mobilise and share knowledge, expertise, technology and financial resources, to support the achievement of the Sustainable Development Goals in all countries, in particular developing countries" by enhancing the global partnership for sustainable development, ensuring harmonised perspectives on technological development, while promoting cohesiveness and cooperation within and between countries.

Policy action 4.3 tries to reducing the cybersecurity skill gap, which is addressed in target 4.4 "By 2030, substantially increase the number of youth and adults who have relevant skills, including technical and vocational skills, for employment, decent jobs and entrepreneurship".

CONTEXT

Trust in today's digital environment plays an important role and is intertwined with concepts like reliability, quality, and privacy. Between 2012 and 2021, global trust in the tech sector has dropped from 77% to 68%. The public has become increasingly suspicious of tech with things like misinformation, personal privacy, 5G networks, and AI bias topping the list of worries[94].

The societal norms and objectives that digital trust is intended to promote and safeguard have safety at their core. This is especially important now as the COVID-19 pandemic forced millions of people into the habit of telemedicine, remote work, online education, and e-commerce. Individual consumer purchasing decisions are directly correlated to digital trust. On a national and even global scale, digital trust supports and enables economic growth. As the world economy grows increasingly dependent upon 'always-on' connectivity, data exchange, and technological innovation digital trust is increasingly becoming fundamental for all parties.

The increase of global interconnectivity in the wake of digital transformation across the world and the advent of the Fourth Industrial Revolution has resulted in increasing security threats that significantly undermine trust[95]. If it were measured as a country, then cybercrime may be the world's third-largest economy after the U.S. and China[96]. This is because, in 2023, the cost of cybercrime is predicted to touch USD 8 trillion[97]. Moreover, cybercrime is getting more sophisticated with time, with the perpetually running cycle of cyber criminals advancing their means as cyber defenses get stronger, and vice-versa. As per the World Economic Forum's World Cybersecurity Outlook 2022, "cybercriminals are seizing every opportunity to exploit vulnerabilities against people and organisations through technology.

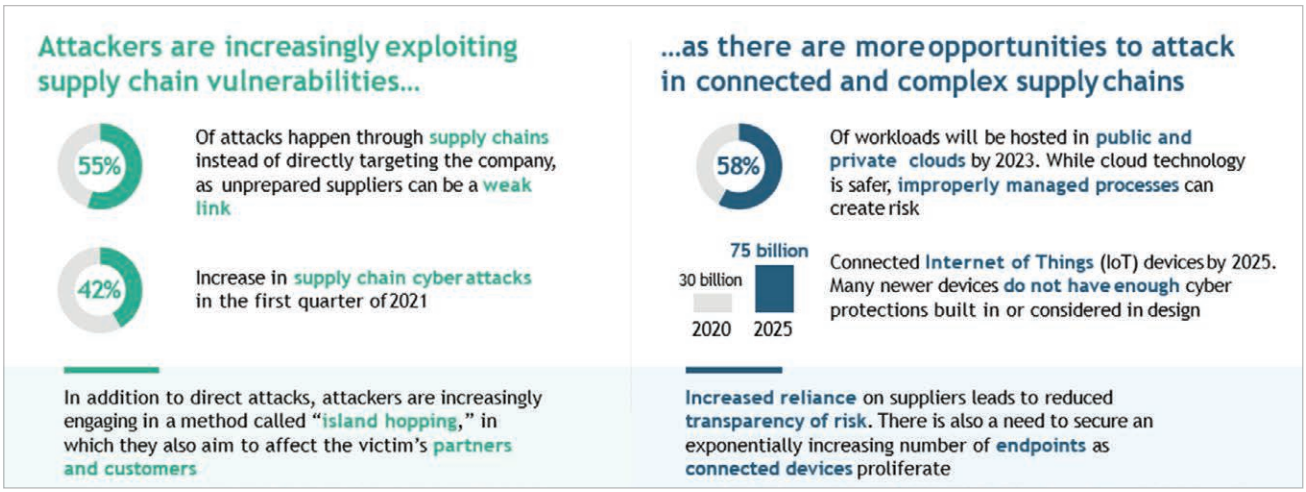
94 World Economic Forum, Explainer: Why we must rebuild digital trust for a cyber-inclusive future?, 2021
95 World Economic Forum, Explainer: As cybercrime evolves, how can companies keep up with their cybersecurity?, Nov 2021
96 Cybersecurity Ventures, Special Report: Cyberwarfare In The C-Suite, 2021
97 Cybersecurity Ventures, Official Cybercrime Report 2022

They are more agile than ever; swiftly adapting new technologies, tailoring their attacks using novel methods and cooperating closely with each other."

Cybercrime affects both the public and private entities both, as well as the society at large. Businesses, for which information drives a large portion of value generation with information passing through many interconnected systems, are at higher risk of an attack, with more severe consequences[98]. Those businesses that process and store large amounts of customer and financial information (for example, credit card companies) are also more prone to being targets of cyber criminals.

In spite of how strong defenses are built, cyber criminals are able to find a way in, for example by exploiting weak links in the chain. Small and mid-size enterprises (SMEs) connected to an organisation's network are often used as a weak link and represent most vulnerabilities. They have increasingly become a target of cyber-attacks. As per a WEF Global Cybersecurity Survey[99], 88% of respondents expressed concern over the resilience of SMEs within their ecosystem. Many of the smaller businesses lack the budget and skills necessary to adequately safeguard their online or point-of-sales ecosystems, making them popular targets. Vulnerable SMEs are largely seen as a key threat to supply chains, partners networks and related ecosystems[100].

Exhibit 11: Increasing exploitation of supply chain vulnerabilities



Source: CEO's Guide to Cybersecurity, BCG

Compliance

Most organisations dealing with data and with a heavy dependence on digital systems have formal processes in place to safeguard their systems. Earmarked cybersecurity budgets are used for a variety of purposes right from employee training to strengthening systems through investing in security controls. A crucial and significant element of cybersecurity budgets is compliance, which refers to adherence to regulations and frameworks while subscribing to best practices.

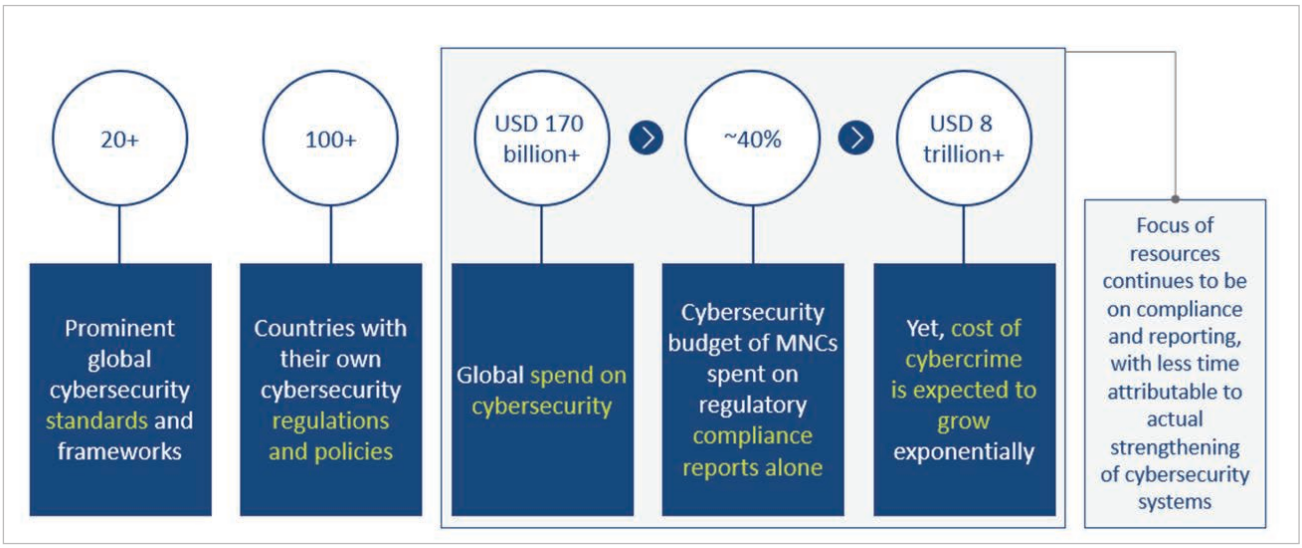
There are over 20 different cybersecurity standards across the world that lay down best practices and guidelines for cyber risk management, NIST and ISO 27001 being some of the prominent ones. Although not mandatory or enforceable by law, compliance with most of these standards requires a significant degree of time and effort investment. On top of these standards, over 150 countries have their own respective frameworks and requirements (legislations) around cybersecurity, that require adherence[101].

98 BCG, Cybersecurity Meets IT Risk Management: A Corporate Immune and Defense System, 2018

99 World Economic Forum, Global Cybersecurity Outlook, 2022
100 World Economic Forum, Global Cybersecurity Outlook, 2022
101 Unctad.org, Cybercrime Legislation Worldwide, https://unctad.org/page/cybercrime-legislation-worldwide

This multitude of requirements with limited-to-no harmonisation amongst them leads to organisations having to spend a major portion of time and resources on compliance alone, reducing their ability to actually focus on strengthening systems and monitoring risks. Over 40% of cybersecurity budgets are generally spent on compliance reporting alone[102]. The average cost of compliance for organisations varies significantly by industry, starting from USD 5 million[103], with most of the funds allocated to specialised technologies, incident response, audit and assessment requirements, security controls and people. In addition to the 40% monetary spend on compliance, it is estimated that Chief Information Security Officers (CISOs) of organisations also often tend to spend over 40% of their time overseeing requirements of compliance with standards and regulation - a sub-optimal use of capacity[104]. Despite these investments, organisations are unable to adequately and effectively subvert risks.

Exhibit 12: Increasing cost of cybercrime in spite of numerous standards and regulations



Source: United Nations; Forbes; IBM – Cost of Data Breach Report 2022; BCG analysis

Non-compliance and implications of cyber-infringements

The global sector spend on cybersecurity is estimated to have exceeded USD 170 billion in 2022 and is expected to continue growing at a compound annual growth rate (CAGR) of ~9% till 2027[105]. Despite the quantum of resources poured into maintaining the sanctity of systems, the cost of cybercrime is expected to continue growing exponentially. In 2023, the global cost of cybercrime is expected to be ~USD 8 trillion, pegged to grow to USD 10.5 trillion by 2025[106], affecting all - private and public sector organisations as well as individuals at large.

IBM's Cost of Data Breach Report highlights that the average cost of a data breach for an organisation stood at USD 4.35 million in 2022. The report lays down 4 key components of the cost of a data breach:

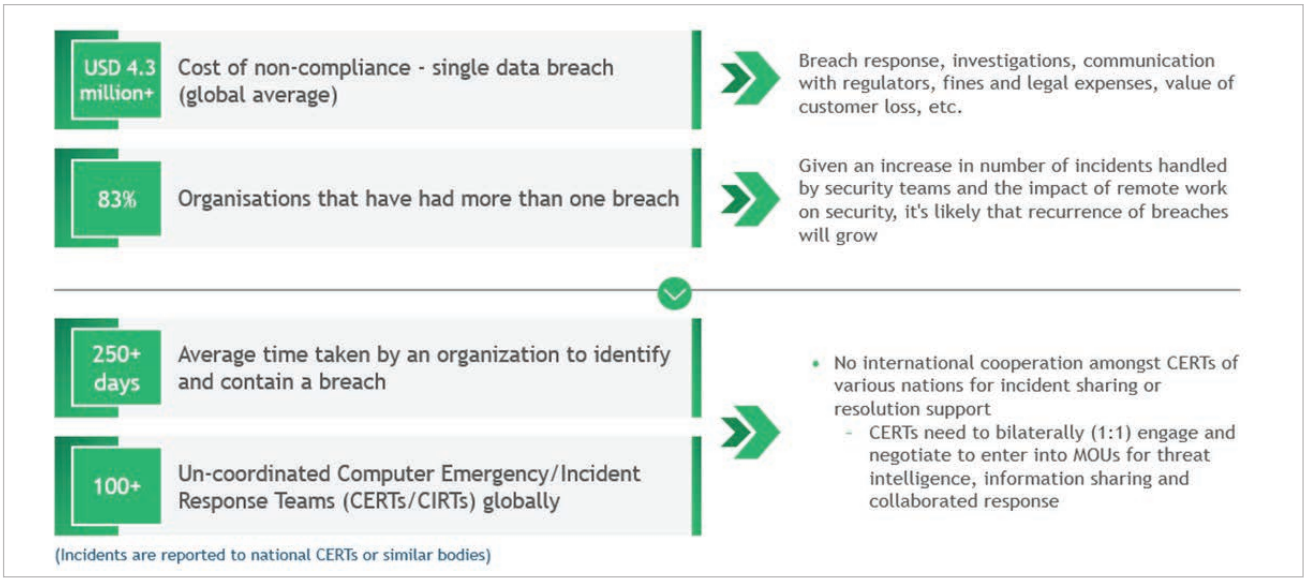
- **Detection and escalation:** Includes forensic investigations, audits, and communication to management

102 Forbes, Cutting The Cost And Complexity Of Cybersecurity Compliance, 2022
103 Ponemon Institute LLC, True cost of compliance with Data Protection Regulations, Dec 2017, a study of select multinational organisations
104 BCG analysis; Birlasoft.com, Top Mistakes Financial Services Firms Must Avoid: Transforming Cybersecurity Compliance, Banking Policy Institute 2021; Cyber Risk Institute 2018, https://cyberriskinstitute.org/industry-unveils-cybersecurity-profile/
105 Markets and Markets, Market research report on Cybersecurity Global Forecast, August 2022 https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html; Statista, Cybersecurity market revenues worldwide 2021-2027
106 Cybersecurity Ventures, Official Cybercrime Report 2022

- **Notification:** Includes complying with regulatory requirements and communication to a broader set of stakeholders
- **Post-breach response:** Includes legal processes, regulatory fines, and customer management
- **Lost business:** Considers the impact of disruption on business

The initial stage of identifying a breach alone takes organisations 200+ days on average. Breaches are often not caught by Security Operations and Control (SOC) teams through regular monitoring processes and are only discovered when data turns up on the darknet or chatter is caught by independent cybersecurity experts. Moreover, the containment stage takes organisations 50+ days on average[107] – to manage all stakeholder communications and safely restore system backups.

Exhibit 13: Cost of data breach and incident response methodology



Source: IBM's Cost of Data Breach Report 2022; ITU; BCG analysis

The WEF's Global Risk Report 2022 puts cyber risk as one of the top 10 global risks. However, it is the only area still without adequate dialogue, multilateral cooperation or coordinated focus. Moreover, the cybersecurity value chain is fragmented with a wide range of stakeholders responsible for diverse tasks:

- **Standard setting bodies:** Bodies like NIST and ISO issue standards that serve as guidelines for best practices in cyber preparedness and managing cyber risks
- **Policymakers:** National regulatory authorities formulating regulations around cybersecurity and data protection
- **National cybersecurity agencies:** Bodies like CISA (of the US) are responsible for leading cyber defense cooperation within the nation and protection of critical infrastructure
- **CERTs:** Most nations have designated Cybersecurity Emergency Response Teams (CERTs) (100+ across the world) that have varying mandates ranging from incident response support to maintaining relationships with other CERTs for proactive coordination in the event of a data breach
- **Threat reporting bodies:** Not-for-profit alliances like FIRST and Cyber Threat Alliance try to bring together a wide variety of security and incident response teams including in particular product security teams from the government, commercial, and academic sectors to exchange best practices and bring larger cooperation around responding to threats
- **Cybercrime enforcement:** Nations typically have cyber cells within their police forces with agencies like Interpol handling cross-border cases

107 IBM, Cost of Data Breach Report, 2022

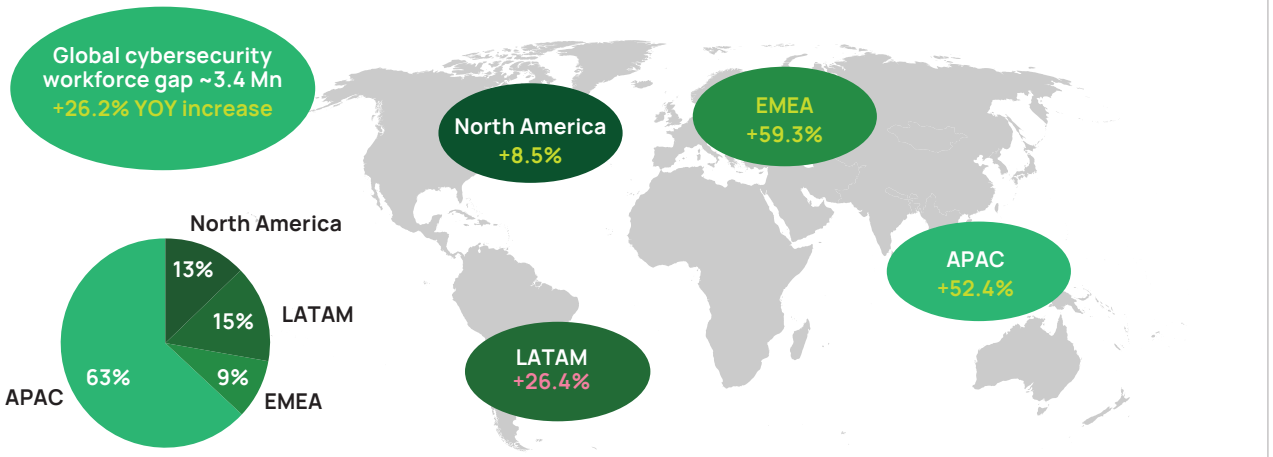
All these stakeholders operate independently with limited-to-no coordination among them. This not only makes compliance processes more tedious for organisations but also limits the potential for speedy resolution in the event of a breach.

In addition to businesses, critical infrastructure of nations is increasingly becoming a target of cybercrime. This constitutes financial services ecosystem, dams, energy generating plants, transport infrastructure, and digital public infrastructure platforms, amongst others. There has been an increase in the percentage of attacks on critical infrastructure – from 20% of nation-state notifications to 40%. The average cost of a data breach for critical infrastructure organisations was ~USD 5 million in 2022 — USD 1 million more than the average cost for organisations in other industries. Cyber-secured critical infrastructure and digital public platforms are vital for national security, better governance, and more importantly, retaining citizens' confidence. Hence, we suggest the following policy actions.

Cybersecurity skill gap

Despite increasing threats and costs, global readiness on the topic is not keeping the same pace. Companies are not always at par in terms of security standards and procedures. This can also be attributed to a worldwide deficit regarding cyber security competencies resulting in a gap of 3.4 million people[108]. The cybersecurity workforce gap has grown more than twice as much as the workforce, with a 26.2%[109] increase in 2022 compared to 2021, making it a profession in dire need of more people. More than half of the employees at organisations with a workforce shortage feel that staff deficits put their organisation at a "moderate" or "extreme" risk of cyberattack. A WEF survey[110] found that 59% of all respondents would find it challenging to respond to a cybersecurity incident due to a shortage of skills within their team.

Exhibit 14: Global cybersecurity workforce gap across 4 regions



APAC contributes to ~63% of workforce gap, and has observed a YoY increase of 52.4% workforce gap from 2021 to 2022

Source: (ISC)² Cybersecurity Workforce Study 2022

108 World Economic Forum, Cybersecurity workforce study by (ISC)2, 2022, https://www.isc2.org/Research/Workforce-Study#, https://www.weforum.org/agenda/2022/12/how-boosting-diversity-cybersecurity-skills-gap/

109 (ISC)² Cybersecurity Workforce Study,2022, https://www.isc2.org//-/media/ISC2/Research/2022-Work-Force-Study/ISC2-Cybersecurity-Workforce-Study.ashx

110 World Economic Forum, Global Cybersecurity Outlook, 2022

There have been some efforts and developments in recent years to strengthen cyberspace regulations and improve global cooperation. However, more needs to be done.

There is a need to foster greater multilateral cooperation around cyberspace and enable wider trust around digital systems and processes. B20 in 2022, under the Indonesian Presidency, had discussed that it is imperative to facilitate Data Free Flow with Trust (DFFT). Despite an increased need for data and evidence of its economic and social advantages, data access and sharing have yet to reach their full potential. In order to promote DFFT, we would require enhanced cybersecurity, compliance with national data protection regulations, and international cooperation on intellectual property rights – aimed to strengthen trust among the countries.

B20 India hopes to take forward Indonesia's recommendations and bring the attention of G20 leaders to this critical global challenge of cybersecurity, bringing greater stakeholder engagement and multilateral cooperation. Addressing these concerns will require a global coordination of effort across public and private sectors to think more expansively about their roles in the digital trust ecosystem.

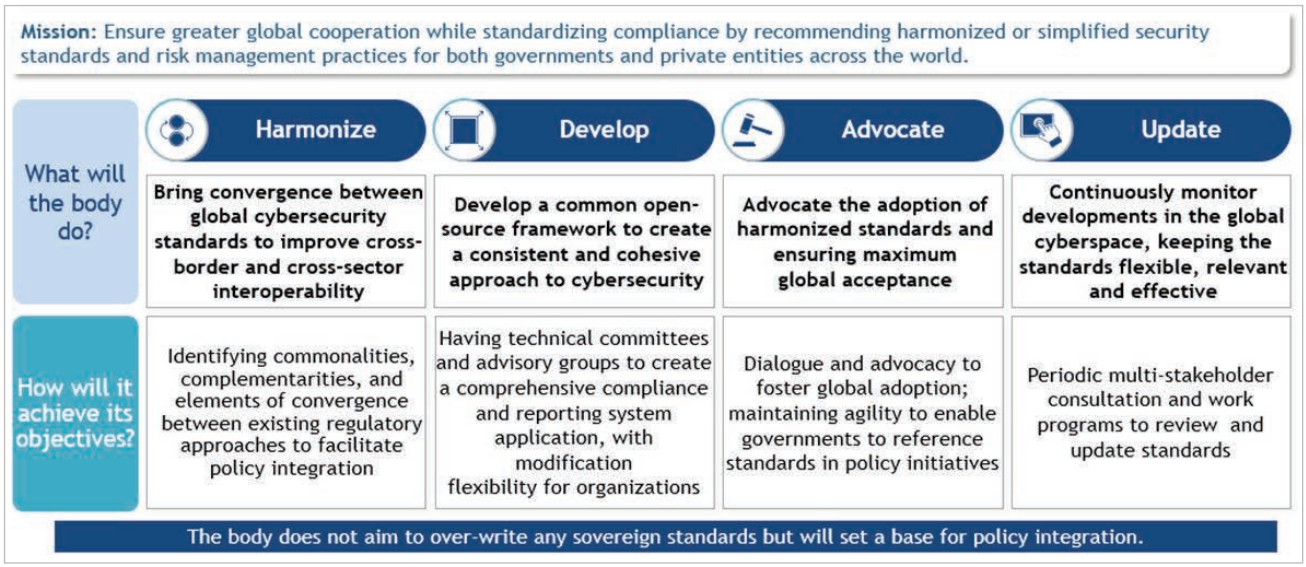
In an effort to guide G20 towards creating digital trust in the ever-changing cyber landscape, the B20 Digital Transformation Task Force seeks to draw attention towards the following policy actions:

Policy Action 4.1: Institutionalise a global body with a mandate of harmonising and advocating cybersecurity standards and bringing in a greater degree of multilateral cooperation

Over 150 nations have their own cybersecurity and data protection regulations, making it especially difficult for MNCs to navigate the web of multiple intersecting and overlapping laws. Several nations are still in the process of developing their own frameworks. Since regulation is a sovereign subject, the body would not mandate standardisation of laws but would provide policy recommendations and technical support to nations aligning their respective regulations and making them as globally harmonised as practicable.

From both a monetary and non-monetary perspective, the threat and impact of cyber infringements can be significantly reduced through greater multilateral cooperation across avenues. Hence, the proposed body would aim to bring in coordination in setting standards and best practices along with cooperation in ensuring that international preparation within the cyberspace is agile and ahead of the evolving cyberspace.

Exhibit 15: Setting up of a global body on cybersecurity



Objective

- Ensure convergence between global cybersecurity standards to improve cross-border and cross-sector interoperability
- Develop a common open-source framework to create a consistent and cohesive approach to cybersecurity and improve global ease of doing business
- Advocate the adoption of harmonised standards and ensure maximum global acceptance
- Continuously monitor developments in the global cyberspace and keep the standards flexible, relevant, and effective

Detailed description of the role

1. Harmonisation of standards

As we have already seen, over 40% of cybersecurity budgets are typically spent on compliance reporting alone. There are over 20 different cybersecurity standards across the world laying guidelines for cyber risk management - NIST, ISO 27001, and CIS 18 are some of the prominent ones. Although individually comprehensive in their own respect, there is a lack of harmonisation amongst such standards with each setting their own guidelines at varying levels of depth. A cross-country comparison can reveal the magnitude of the problem faced by businesses in terms of adhering to a vast number of non-harmonised frameworks (country, industry and sector specific) and regulations.

The way forward is to establish trust and promote international inter-operability of risk-based security and privacy protection standards across jurisdictions. To achieve this, the body will have the harmonisation of standards as one of its key mandates, bringing varying guidelines together to create a single and consistent framework for organisations to follow. This would create a comprehensive compliance and reporting system based on security requirements and needs in various industries. The body should also accord adequate flexibility to allow organisations to only follow standards directly applicable to them. Further, this set of standards should be open source, allowing other bodies and nations across the world to adopt the same with desired modifications.

2. Development of open-source framework

The body's primary goal under its mandate will be to create an open-source framework, a universal language, and a methodical approach to managing cybersecurity risk. The framework's main components will comprise activities that may be added to a cybersecurity programme to make it robust as well as provide flexibility to organizations in its adoption. The standards will be created to support, not replace, a company's risk management and cybersecurity programme. The framework must be sufficiently adaptable even though it will be created with critical infrastructure and cyber priorities of all stakeholders in mind. The body should ensure that the framework has built-in modification capabilities so that it can be tailored for usage by any sort of organisation with varied domains, scales, or levels of maturity. It ought to be beneficial to both businesses that are just starting to build cybersecurity programmes and those that already have established programmes. The G20 nations should aim to do so through technical committees and advisory groups within the body that help create a single window compliance and reporting system with application and modification flexibility for organisations.

3. Advocating the adoption of standards, ensuring global acceptance

To encourage adoption, it is important to collaborate with different stakeholders, including governments, regulatory bodies, industry associations, and standardisation organisations. Open dialogue and constructive engagement can help to build trust and consensus around the benefits of harmonised standards and their potential impact on organisational well-being. Many stakeholders may not be aware of the benefits of harmonised standards or may have misconceptions about their implementation. Awareness campaigns, engagement initiatives and outreach to international bodies can help to address these gaps in knowledge and build support for harmonised standards adoption and ensure that they are adopted globally. Advocates of harmonised standards should provide evidence of their impact in terms of safety, cost benefit and ease of doing business, among other areas.

This can help to convince stakeholders that the benefits outweigh any potential costs. This will also bring the body closer to its aim of maximum policy integration by governments and other national and international entities referring to these standards in their policy initiatives.

4. Updating the framework periodically & maintaining agility of standards

Aligning with the developments in the digital space worldwide, the body will aim at keeping the framework agile and ever evolving. Along with this, the body will have periodic associations with committees comprising of subject-matter experts worldwide representing various sectors. Regular multi-stakeholder consultations and work programs to review and update standards would be undertaken by the body.

As the body matures, it might have the capacity, ability, and flexibility to add several additional mandates to its areas of focus, such as: Bringing together governments, the private sector, and civil society amongst others to engage in collaborative, multistakeholder dialogue. This might become a forum to enable frequent discussions on matters of concern and present a coordinated means to take down cybercrime infrastructure through aligning processes in the event of infringement of cyberspace.

Policy Action 4.2: Improve the trustworthiness of the digital ecosystem and work towards a cyber-inclusive future by advocating cyber-awareness to the grassroots level

~77% of all cyberattacks are caused by human negligence or error and not technological failures[111]. Being vigilant of cybersecurity in everyday situations is referred to as cybersecurity awareness. Cybersecurity awareness includes understanding the risks associated with online interaction, email checking, and web browsing. Most of the current cybersecurity knowledge focuses on protecting the intricate digital infrastructure of big businesses. Giving the typical user, the in-depth knowledge and skills necessary to protect their personal information or a small business system is given much less focus. Cyber awareness is crucial but knowing is not doing. To better understand, comply with and think critically about the digital dangers and solutions which influence their organisations, business owners, especially SME entrepreneurs, need to participate in digital upskilling programs and facilitate cybersecurity talks. Applying a forward-thinking lens, we must bring the future of cyber space into a sharper focus.

1. G20 nations should focus on educating the larger community about digital safety and spread awareness about preventive and curative actions required to be taken in response to the threats that exist in the cyberspace

The G20 countries should focus on multilateral efforts towards public awareness campaigns that educate the public about cyber threats and give them the tools they need to stay safer and more secure online. Each stakeholder has a responsibility to contribute to the shared goal of cybersecurity. Being a part of the digital world becomes safer for everyone when we all take small efforts to be safer online, whether at home, at work, or in our communities. Governments, business, and nonprofit organisations should be encouraged to work together to promote secure online conduct and practices and increase global cybersecurity awareness standards.

1a. Organise global public campaigns, support private initiatives, and leverage media channels to ensure that each section of the society learns about cyber awareness with practical and real-life understanding of the issue

To ensure gender-parity and geographic and socio-economic inclusion in imparting of cyber-safety knowledge, G20 nations must align with stakeholders responsible for interacting with each of these groups. A few steps towards making cyber-education inclusive could be:

- **Develop a clear message for the right target audience:** Understanding the specific needs of each group, which may include individuals, businesses, government agencies, schools,

111 BCG, CEO's Guide to Cybersecurity, 2021

and other organisations will help tailor the message and develop an approach essential to communicate the importance of cyber awareness. It should be practical and relevant and must emphasise the real-life consequences of cyber threats

- **Partner with private organisations and media channels:** Organisations that have expertise in cybersecurity can help provide more resources and credibility to any such campaign. These organisations may include cybersecurity firms, IT service providers, and other tech companies. Both traditional and new-age media channels should be leveraged to the full extent to ensure maximum dissemination of information
- **Resources accessibility:** Providing resources such as online or field training courses, guides, and checklists can help individuals and organisations take practical steps to improve their cybersecurity. These resources should be easily accessible and customised basis the abilities and needs of the receiving end

1b. Initiate educational training programmes focusing on youth to impart knowledge about identifying and mitigating risks in the digital space

With rising levels of education and penetration of mobile and internet devices, the tech savvy young population often considers itself to be digitally immune. There are more than 5.3 billion mobile devices worldwide and with rising security threats, mobile devices are accounting for more than 60% of digital frauds[112]. 20% of GenZers and 18% of Millennials have had their identity stolen at least once[113]. Despite the increasing cyber threats, the global cybersecurity workforce gap stands at around 3.4 million[114].

G20 nations should encourage multi stakeholder collaboration on upskilling people within the cyberspace. Specialised programmes with a forward-looking approach in the area of cybersecurity should be designed possessing the following agenda:

- Hands-on-training in the fundamentals of cybersecurity through realistic security simulations
- Impart knowledge on ability to harness new technologies and aim to equip citizens globally with appropriate tools to counter cyber threats
- Guidance on how to recognise and combat misinformation and disinformation, as well as information on mechanisms to report the same
- Promote career paths and upskilling initiatives within cyberspace and security operations highlighting the opportunities and scope that lie within the knowledge area

2. G20 countries should adopt norms and practices to safeguard people's data and build trust among all stakeholders, focusing on MSMEs' cyber-preparedness and addressing inhibitions towards digitisation

Making digital technologies trustworthy is a critical subject to consider in a time when they are essential to every element of business progress and social interaction. As per a study by the European Union Agency for Cybersecurity, 45% of SMEs in EU implemented new technologies during the pandemic but over 90% did not implement any mechanisms to ensure the security of these solutions[115]. Popular notion about digital trust is that digital products and services, as well as the companies that deliver them, will serve the interests of all stakeholders. Moreover, small and large organisations have also laid trust upon these technologies, making digitisation a backbone of many business entities.

Now that most firms run on digital platforms and new technology and techniques emerge every day, new types of cyber threats also do so quickly. It is crucial since any breach of a company's digital trust can have a detrimental effect on the success of the company as well as the customer experience and brand reputation. As per an OECD report, SMEs spend much less than is optimal on

112 Cyber Security Almanac, 2022

113 National Cybersecurity Alliance, Annual Cybersecurity Attitudes and Behaviors Report, 2022, https://20740408.fs1.hubspotusercontent-na1.net/hubfs/20740408/CYBSAFE-Oh%20behave%20report%202022-220927%20MS%20-%20V1.pdf?utm_campaign=Cybersecurity%20Awareness%20Month&utm_medium=email&_hsmi=227714065&_hsenc=p2ANqtz-_x84uFF6YLxinYFuJ6F39i3A2WyzVP1ayG0YPPgg_Sg5VXhKZ1-yEz7QV6iE_Hr6YwYfvgTv1hMRtYv25n79Bu0x4InQ&utm_content=227714065&utm_source=hs_automation

114 (ISC)2 Cybersecurity Workforce Study,2022, https://www.isc2.org//-/media/ISC2/Research/2022-Work-Force-Study/ISC2-Cybersecurity-Workforce-Study.ashx

115 ENISA, Cybersecurity For SMEs, June 2021

their digital security strategy, with over 50% indicating they would not spend more than Euro 250 annually[116]. For organisations aiming to inspire confidence among their customers, employees, and partners that online business processes and interactions are secure, identity, integrity, and encryption are crucial building elements.

2a. Facilitate fulfilling of cyber compliance requirements by MSMEs and streamline the process of technical upgradation through necessary training and maintenance support

MSMEs often need education and training on cybersecurity best practices, including password management, phishing awareness, and data protection. Governments, industry associations, and digital service providers can offer training programs and resources to help MSMEs become more knowledgeable and vigilant in identifying and mitigating cyber threats. Collaborative efforts should be made in form of offering guidance and tools to support MSMEs in keeping their software and systems up to date with the latest security updates and patches to protect against cyber threats.

G20 countries should facilitate programmes, alliances and tools that will lower the cost of cybersecurity solutions for SMEs. For instance, a large number of SMEs use cloud services, which are handled by the provider in accordance with standardised contract provisions and Service Level Agreements (SLAs). Due to their small size, individual SMEs cannot negotiate appropriate SLAs, although larger companies may be able to do so. SMEs in bigger numbers may create specialised SLAs or contract conditions by pooling demand to better suit their cybersecurity needs[117].

2b. Support MSMEs in formulating incident response plans to ensure that digital trust of all stakeholders is upheld even during direst cyber-situations

An incident response plan mitigates the risk of a cyber-attack. With a thorough plan in hand, business owners know that they have a strategy in place to protect their business from cyber-attacks, steps outlined to recover data and systems, and a well-thought-through plan in place to maintain client trust in even the direst situation. Governments and industry associations can offer guidance and resources to help MSMEs develop and implement an incident response plan with following benefits for MSMEs:

- **Disaster preparedness:** The strategy will make sure that an MSME can prioritise the necessary actions for the reaction, map out the resources required for recovery, and manage their staff in the face of the attack by anticipating potential dangers and the necessary responses in advance
- **Protecting stature:** The purpose of having a curative strategy in place is to guard against brand deterioration and legal action for MSMEs. Clients and partners may end contracts and look for new service providers if an event exposes their personal data. That costs the company a fortune and could impact its future growth
- **Rapid response:** An MSME will be ready to implement a plan as soon as an attack is discovered. Employees will feel empowered by the plan and be able to trust the recommended operational activities. Thus, they will not forget any crucial tasks and will know exactly what to do and when. It will also make it possible for a team of responders to notify important parties about the crisis.

2c. Incentivise and educate MSMEs regarding cyber insurance to help MSMEs protect themselves against potential losses due to cyber-attacks

Intended to protect businesses from threats related to IT infrastructure and activities, cyber insurance safeguards MSMEs from the first and third-party costs associated with a cyber breach. In the 2019-2021 period, even though cyber insurance claims grew by 100%, and 56% of the cyber claims were arising from SMEs[118], total number of SMEs aware of or adopting cyber insurance was significantly low. Conventionally, the firm ultimately bears responsibility when a breach occurs, and data is destroyed. Penalties, fines, or even legal action may be imposed as a result of this. This demonstrates how neglecting secure measures to safeguard sensitive information bears repercussions for MSMEs.

116OECD, Digital Security and Data Protection in SMEs, October 2020
117 ENISA Cybersecurity For SMEs, June 2021
118 Astra Security Report, 2023

118 Astra Security Report, 2023

G20 nations must take a significant part in narrowing the protection gap and creating a system of strategic risk sharing that strengthens community financial stability and resilience, with respect to growing cyber threats. G20 countries must put their efforts into creating an ecosystem with the right organisations and agencies that are accredited to identify and certify such losses in the digital space, to provide MSMEs seamless access to cyber insurance.

Policy Action 4.3: Bridge the cybersecurity skill gap by facilitating faster development of cyber talent pipeline through increased investment in existing cyber-skilling institutes, complemented by building national cyber academies, through the public-private partnership route

1. G20 countries should empower cyber-skilling institutes with the tools and resources required to attract talent and provide training and employment opportunities in partnership with the industry; this could also be complemented by setting up of National Cyber Academies, which can help bridge this skill gap through targeted interventions

Government commitment to create awareness and prepare the upcoming generations for a cybersecure world is very important. Several private organisations have also taken steps in this regard and have launched national skilling campaigns to fill the cybersecurity jobs by helping community colleges, partnering with global organisations, and providing free resources and tools for teaching. However, despite such efforts, the world sees an immense cybersecurity skill gap, with over 3 million cybersecurity professionals needed across the world today.

This calls for heightened engagement with multiple stakeholders, primarily the educational and cyber-skilling institutes. Creating interest about the profession among students, starting at the middle-school and higher secondary levels, is crucial to attract them into the field. Governments can collaborate with existing institutes to explore opportunities to promote awareness forums with educational entities, directly fund high-school and university programs, and partner with top tech companies to run education programs and offer internship/placement opportunities. Existing institutes can also partner with industry to receive continually upgraded research and teaching support through consultation on course material, guest lectures, and research projects for students.

In addition to supporting existing institutes, government can explore setting up National Cyber Academies, to further increase the supply of cybersecurity professionals through targeted interventions, especially in regions with no specialised institutes.

These academies can provide self-paced learning to both students and employees in a cost-effective and agile manner. Further, they can provide certified training programs aligned to international cybersecurity frameworks and standards, such as NIST, and capture industry best practices into the course curriculum. This will enable accelerated career development for professionals, both for early and advanced practitioners.

These academies can collaborate with industry to help prepare candidates for career pathways, leverage industry knowledge to update course curriculum and provide mentorship and create personalised programs for companies hiring for specific skills.

At a macro level, these national academies can help support countries in devising their cybersecurity skilling and education strategies and curriculums, derived from on-ground best practices and learnings.

Task Force Members

Name	Organization	Country
Aleksandr Sergeevich Suraev	The Russian Union of Industrialists and Entrepreneurs (RSPP)	Russian Federation
Abdiansyah Prahasto	Deloitte	Indonesia
Abhay Deshpande	Recykal	India
Ahmed M Kouther	Mind Stream Group	Saudi Arabia
Aiman Ezzat	Capgemini	France
Ali Akhtar Jafri	MAIT	India
Amit Marwah	NOKIA NETWORKS	India
Amur S Lakshminarayanan	Tata Communications Limited	India
Anant Maheshwari	Microsoft Corporation India Pvt. Ltd	India
Andrey Andreevich Filippov	Digital Economy ANO	Russian Federation
Andrey Bugrov	Norilsk Nickel	Russian Federation
Andrzej Przewiezlikowski	Comarch	Poland
Andy Song	eNotus International Inc.	Australia
Ankit Agarwal	Sterlite Technologies	India
Annapurna Vishwanathan	Cummins India Limited	India
Anurag X Gupta	Accenture	India
Apratim Mukherjee	KPMG	India
Arief Gunawan	Telkom Indonesia	Indonesia
Arrizka Faida	Cornell University	Indonesia
Atul Hemani	1008 Digital Health Pvt. Ltd.	India
Avijeet Dutta	Globant	India
Barbara P. Wanner	U.S. Council for International Business	United States
Barbara Ubaldi	OECD	Estonia
Bishakha Bhattacharya	Amazon Web Services India	India
Bryan Saragih	ASEAN Your Organization	Indonesia
Carsten Alexander Lexa	Lexa Legal	Germany
Caterina Bortolini	TIM	Italy
Chander Prakash Gurnani	Tech Mahindra	India
Chandrashekar Bharathi	AceMicromatic MIT (AceMicromatic Group)	India
Chetan J Baregar	Recykal	India
Chetan Krishnaswamy	Amazon Seller Services Private Limited	India
Christoph Seydel	Mededis GmbH	Germany
Daniel Pujazón	PagoNxt (a Santander company)	Spain
Danilo Gismondi	Autostrade per l'Italia SpA	Italy
Darhl Gregory Vercaigne	VCMx Exchange Inc	Canada
Dario Pagani	Eni s.p.a.	Italy
Dariusz Tomasz Prosiecki	Employers Poland	Poland

Name	Organization	Country
Diane Wang	DHgate Group	China
Diane Wang	DHgate Group	China
Dilip Asbe	National Payment Corporation of India	India
Dilip Sawhney	Rockwell Automation	India
Dinora Quadretti	IQT Consulting S.p.A.	Italy
Divyanshu Varshney	VR AR MR	India
Dmitry Vladimirov	JSC ZYFRA	Russian Federation
Eduardo Salido Cornejo	Amadeus IT Group	Spain
Erwandi Hendarta	Baker McKenzie/HHP	Indonesia
Evgeny Igorevich Melnikov	Russian Union of Industrialists and Entrepreneurs	Russian Federation
Fabio De Felice	Protom Group S.p.A. a socio unico	Italy
Federico Dell'Aquila	Argentina Chamber of Commerce and Services	Argentina
Ganesh G Natarajan	Honeywell Automation India Ltd & 5F World Pvt Ltd	India
Gaurav Malik	Successive Technologies	India
Genie Sugene Gan	Kaspersky	Singapore
Georgina Lv	DHgate	China
Gillian Crossan	Deloitte	United Kingdom
Gustavo Oliveira	T3 Asset Management	Brazil
Col Haridas M	DataVal Analytics India Pvt.Ltd.	India
Heba Shams	Mastercard	Germany
Dr. Holger Bingmann	Bingmann Pflüger International	Germany
Howie Lau	SGTech	Singapore
Huajing Huang	China Council for the Promotion of International Trade Guangxi Committee	China
Isa Antariksa	PT PERTAMINA (Persero)	Indonesia
Jana Junele	Wirk World LLP	Latvia
Javier Alberto Bolzico	Asociacion de Bancos Argentinos ADEBA	Argentina
Jing Zhu	Alibaba Group	China
Juan Luis Redondo Maillo	Telefonica	Spain
Kanti Dugar	MediaJade	India
Kapil Murlidhar Sharma	Microsoft India Private Limited	United Kingdom
Kevin Wu	Talent Box	Indonesia
Klemens Kober	DIHK - Association of German Chambers of Commerce and Industry	Germany
Koh Nakajima	Keidanren (Japan Business Federation)	Japan
Kristen Lee Robinson	Open Contracting Partnership	United States
Kulmeet Bawa	SAP India Pvt Ltd	India
Kunal Bahl	Snapdeal Limited (AceVector Group); Titan Capital	India

Name	Organization	Country
Lalitha Mohan	Azbil Corporation	Singapore
Leigh Howard	Asialink Business	Australia
Liang Xu	CCOIC	China
Liudmila Renne	Joint Stock Company "Russian Railways", JSCo"RZD"	Russian Federation
Louisa Tomar	Center for International Private Enterprise	United States
Lovneesh Chanana	SAP Asia Pte. Ltd.	India
Lynnette Nontobeko Magasa	Boniswa Corporate Solutions/Boniswa Group	South Africa
Mandeep Kohli	Boston Consulting Group	India
Manish Sharma	Bluwage	India
Manish Sharma	Bluwage	India
Marianne Coutinho	KPMG	Brazil
Martín Gonzalo Umaran Sanchez	Globant	Argentina
Martin Schroeter	Kyndryl	United States
Martine Allaire	ORANGE	France
Mashael Abdullah Bin Saedan	Al Saedan For Development	Saudi Arabia
Maxence Demerlé	MEDEF	France
Meena Shah	iView Labs Pvt Ltd	Indian
Michael Harvey	Canadian Chamber of Commerce	Canada
Michalina Seliga	Embassy of Poland in New Delhi	Poland
Michelle Chivunga	Global Policy House	United Kingdom
Mohamed Zaki Elsewedy	Federation of Egyptian Industries	Egypt
Mohammed Soliman Mosly	SEDCO Holding	Saudi Arabia
Naga Ramaneshwar	PVM Innvensys Private Limited	India
Nguyen Khuong Duy	World Group	Vietnam
Nicklas Bert John Jonow	Pacific Consulting Group (Asia) Ltd	Sweden
Nitin Narayan	Mavenz Management and Technology Services Pvt Ltd	India
Norberto Capellán	Cámara Argentina de Comercio y Servicios	Argentina
NSN Murty	Deloitte Touche Tohmatsu India LLP	India
Olga Kayayan	Boniswa Corporate Solutions/Boniswa Group	France
Orlando Taddeo	Mexedia	Italy
Panish Hangal	Larsen & Toubro (Smart World and Communication Unit)	India
Paulino G Lagunes Aguirre	Grupo Jaran S.A. de C.V.	Mexico
Peter Spivack	Hogan Lovells	United States
Pingping Ren	iFlytek CO.LTD.	China
Podbiralina Galina Victorovna	Federal State Budgetary Educational Institution of Higher Education Russian University of Economics. G.V. Plekhanov"	Russian Federation

Name	Organization	Country
Pranjal Sharma	Self Employed	India
Dr Prashant Pansare	Rubiscape Pvt Ltd	India
Prem Prakash Dalua	TVS Motors	India
Prerna Saxena	Better Than Cash Alliance/ United Nations Capital Development Fund	India
Purushottam Kaushik	World Economic Forum	India
Qihong Wang	Zhong Lun Law Firm	China
Quint Andrea Simon	Amazon Web Services	United States
Rabindra Srikantan	ASM Technologies Ltd	India
Ragini Lal	Chipsoft India	India
Rahul Vatts	Bharti Airtel Limited	India
Rajan Jei Anandan	Sequoia Capital India LLP	Sri Lanka
Rajesh Kumar Balasubramaniyam	Avohi	India
Rakesh Verma	Stripe	India
Ramendra Verma	Grant Thornton Bharat	India
Ramesh Jampula	Dell Technologies	India
Ramesh Ramadurai	3M India Ltd	India
Ranjan Bhattacharya	HSBC	India
Ranjeet Goswami	Tata Consultancy Services Ltd.	India
Ratan Shrivastava	BowerGroupAsia	India
Ravi Parkash Gandhi	Reliance Jio & Reliance Retail	India
Ravi Sudhakar Awasarmol	Rashtriya E Shiksha	India
Regina Vianney Ayudya	PT Ardiya Dinara Indotrade	Indonesia
Rishi Mohan Bhatnagar	Aeris Communications India Pvt. Ltd.	India
Rohan Mitra	Adobe Inc	India
Rohan Mitra	Adobe Inc	India
Rohit Srivastava	Dparth Tech Advisory Private Limited	India
S Swaminathan	IRIS BUSINESS SERVICES LIMITED	India
Sachin Suri	CropData Technology Private Limited	India
Sahra English	Citi	United States
Saket Agarwal	Onnivation Ventures	India
Sam Han	Union Communications Hong Kong Limited	China
Samantha Ferreira Cunha	National Confederation of Industry of Brazil	Brazil
Sandeep Girotra	ATC Telecom Infrastructure Pvt Ltd.	India
Sandeep Naik	General Atlantic	India
Sandip Patel	IBM India Pvt. Ltd.	India
Sanjay Nayak	Tejas Networks Ltd.	India
Saravanan Ramdoss	ANT SOLUTION	India
Sarp Kalkan	Union of Chambers and Commodity Exchanges of Türkiye (TOBB)	Turkey
Sergey - Emelchenkov	Zyfra	Russian Federation

Name	Organization	Country
Shaanti Ramchand Shamdasani	S. ASEAN International Advocacy & Consultancy (SAIAC)	Indonesia
Sherbir Panag	Law Offices of Panag & Babu	India
Shipra Dawar	IWill and ePsyclinic	India
Shivnath Thukral	Meta	India
Shivraj Sampatrao Sabale	Globant	India
Shweta Bhardwaj	Johnson and Johnson	India
Srikar Reddy Palem	SONATA SOFTWARE LIMITED	India
Steven Heckler	Federation of German Industry (BDI)	Germany
Subramanya M R	Siemens Technology & Services Pvt. Ltd.	India
Sundeep Vir Narwani	Abris	India
Suresh Sethi	Protean eGov Technologies Limited	India
Swati Rangachari	United Health Group I Optum India,	India
Tedja Somantri	PT TEMARA GLOBAL TEKNOLOGIKA	Indonesia
Timea Suto	International Chamber of Commerce (ICC),	France
Valentina Carlini	Confindustria	Italy
Vaman Desai	BowerGroupAsia	India
Varsha Vibhandik	VV Group	India
Vasily Vasilievich Vysokov	JSC Center-Invest Bank	Russian Federation
Victor Dosoretz	Mantra Beauty SA	Argentina
Vijaykrishnan Venkatesan	Kennametal India Limited	India
Vittoria Carli	Confindustria Servizi Innovativie Tecnologici	Italy
Vivek Sonny Abraham	Salesforce	India
Vladimir Averbakh	Sberbank of Russia	Russian Federation
Weining Guo	Chinamex Middle East Investment & Trade Promotion Centre	China
Willi Hermann	Msg systems ag	Germany
Xin Rui Wang	SHIHUI PARTNERS	China
Yin Yunxia	Fangda Partners	China
Yogesh Soni	Brightside Online Solutions	India
Yong Liu	Qi An Xin Technology Group Co., Ltd.	China
Yuan Yao	CCOIC	China

Network partners

BUSINESS at OECD

OECD
BETTER POLICIES FOR BETTER LIVES

UNITED NATIONS INDIA

Knowledge partner

BCG BOSTON CONSULTING GROUP

About B20 India

Business 20 (B20) is the official G20 dialogue forum with the global business community. Established in 2010, B20 is among the most prominent Engagement Groups in G20, with companies and business organizations as participants. The B20 leads the process of galvanizing global business leaders for their views on issues of global economic and trade governance and speaks in a single voice for the entire G20 business community.

Each year, the G20 Presidency appoints a B20 Chair (an eminent business leader from the G20 host country), who is supported by a B20 Sherpa and the B20 secretariat. The B20 aims to deliver concrete actionable policy recommendations on priorities by each rotating presidency to spur economic growth and development.

The B20 bases its work on Task Forces (TFs) and Action Councils (ACs) entrusted to develop consensus-based policy recommendations to the G20 and to international organizations and institutions. The B20 officially conveys its final recommendations to the G20 Presidency on the occasion of the B20 Summit.

As India holds the Presidency of G20 in 2023, India will host the eighteenth G20 Summit in New Delhi. The Confederation of Indian Industry (CII) has been appointed as the B20 India Secretariat for India's Presidency. CII, as the B20 India Secretariat, will host the B20 India Summit in New Delhi from 25-27 August 2023.

For queries, **reach us at b20secretariat@cii.in**