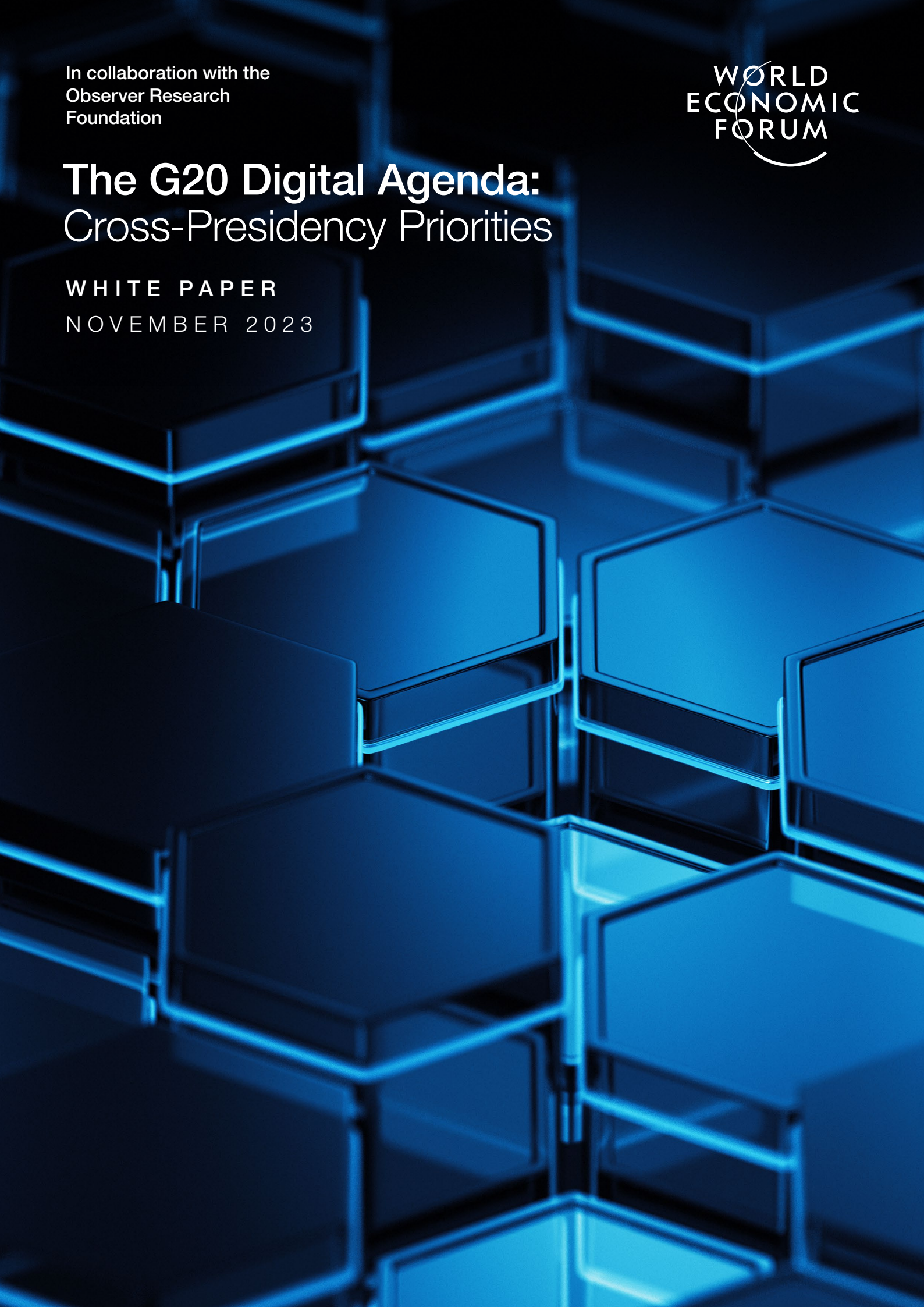
In collaboration with the Observer Research Foundation

WORLD ECONOMIC FORUM

The G20 Digital Agenda: Cross-Presidency Priorities

WHITE PAPER

NOVEMBER 2023



Images: Getty Images

Contents

Foreword

Sebastian Buckup
Member of the Executive Committee, World Economic Forum

Anirban Sarma
Chair, Think20 Taskforce on Our Common Digital Future; Deputy Director, Observer Research Foundation

In May 2023, the World Economic Forum and the Observer Research Foundation (ORF) jointly launched an initiative called Facilitating Cross-Presidency Dialogue on the Digital Agenda for the G20. Its aim was to identify pressing themes the G20 is or should be addressing and support the continuity of engagement around these issues across successive G20 presidencies.

The opportunities identified in this white paper draw on the expertise of business and expert communities convened by the World Economic Forum's Global Future Councils and the Centre for the Fourth Industrial Revolution – a global platform for helping leaders anticipate exponential technologies and accelerate their inclusive and sustainable adoption. It also draws on the substantial body of knowledge and expertise of the ORF, which served as the secretariat to Think20, the G20's official engagement group for think tanks, during the most recent Indian G20 presidency of 2023.

While digital themes have featured on the G20's agenda since the group's formation in 1999, a systematic focus on building a resilient and thriving digital economy came into being in 2016 when the G20 Digital Economy Task Force was created. The following year, the German presidency oversaw the first-ever Digital Economy Ministerial Meeting with an emphasis on a broad spectrum of digital themes, including measuring the digital economy, investing in the ICT sector, promoting digital skills and training, boosting digital entrepreneurship, accelerating digital infrastructure for development, bridging the digital divide and building smart cities. With the establishment of the Digital Economy Working Group under the Indonesian presidency (2022), the focus on digital themes became even more entrenched.[1]

At this point in time, the outgoing, incoming and upcoming presidencies – the so-called G20 Troika – are held by emerging economies. With South Africa slated to succeed Brazil in 2025, emerging economies stand to helm the G20 for four consecutive years. This presents a unique opportunity to place digital access, equity and development at the heart of the G20 agenda.

At a time when the rise of strategic competition and conflicting interests risk hampering collaboration, building consensus around foundational digital norms and technological advancements is crucial. Informing this process is the ambition of this work.

We would like to thank the members of the World Economic Forum's Global Future Councils (GFCs), whose contributions have been critical to this white paper. We hope the paper will support an ambitious and constructive dialogue on our shared digital future.

Executive summary

The G20 digital agenda addresses data protection, digital inclusion, cybersecurity, health, sustainability, infrastructure and global skill development.

The digital agenda priorities of G20 presidencies are often wide-ranging, from the protection and flow of data to bridging the digital divide and making use of technology for development. Each new presidency presents an opportunity to showcase successes and examples from countries that can be scaled across the G20 and globally. The transition between presidencies can also lead to policy gaps in global approaches.

The ever-changing technological landscape brings with it a new wave of challenges and opportunities that require agility and iterative approaches to the global digital agenda. In this context, this paper puts forward key digital agenda themes and recommendations for consideration at the global level, with the hope that these themes and recommendations will be continuously revisited and adapted by the G20 to meet new technological challenges and opportunities:

- **Focusing on the centrality of digital inclusion, access and trust:** To thrive in today's digitally connected world, people, organisations and governments need to interact with a trusted global digital ecosystem.

- **Ensuring cybersecurity of emerging technologies:** Digitization enhances social benefits but introduces cybersecurity risks and challenges, especially from emerging technologies, necessitating robust, globally interoperable cybersecurity policies. A universal baseline for cybersecurity policies and regulatory interoperability among G20 nations is vital for protecting against global cyberthreats, with acknowledgement of challenges from jurisdiction-specific regulations. Similarly, rapid governance standard development and proactive management strategies are needed due to emerging technologies' lack of established best practices and to secure their benefits.

- **Investing in digital health and sustainability solutions:** Both digital health and environmental sustainability are essential pillars of any digital agenda. Leveraging and supporting quality data for digital health and sustainable solutions and driving greater investment in these areas is critical for the advancement of digital solutions.

- **Enabling digital infrastructure**: Data, integral for innovation and economic growth, demands a unified governance approach due to ecosystem variability and growing societal dependence. Cross-border data flows offer expansive opportunities and risks, while digital public infrastructure (DPI) is essential for inclusive digital access, requiring global and multistakeholder engagement.

- **Building digital skills:** Comprehensive digital skilling and upskilling in education and employment are imperative, necessitating varied models and infrastructure to extend technological adoption across roles. There is a need for regulatory capability-building and standardized training frameworks to meet digital workforce demands. This is highlighted by persistent global digital skills shortages and socio-digital disparities, despite available opportunities.

Introduction

The consecutive presidencies of India, Brazil and South Africa in the G20 offer an unparalleled opportunity to advance the G20 digital agenda, especially for emerging economies.

Navigating the complexities of global technology policy, with its entwined implications for privacy, intellectual property and security, necessitates a cohesive, multistakeholder approach to establishing trust within and among communities and countries, even amidst technical, political or social disparities. These efforts should extend beyond the tenure of any one G20 presidency.

The G20 presents a consistent multilateral platform upon which to build cohesiveness in global approaches to technology systems and emerging technologies. Together, G20 members represent 85% of global gross domestic product (GDP), 75% of international trade and two-thirds of the world's population.[2] The G20 is composed of some of the largest countries that stand to benefit from the data-driven digital economy, including the United States and China.[3] Historically, by addressing pivotal technological issues such as digital inclusion and data flows, the G20 has nurtured mutual comprehension, spurred dialogue and amplified cooperation on technology governance among countries with different regulatory regimes.[4] These efforts pave the way for the interoperability of divergent technology policies and standards, facilitating communication among distinct technological systems.[5] The G20 is strategically poised to influence the creation and implementation of global norms around data privacy, cybersecurity and artificial intelligence. It can guide the development of fair and inclusive digital infrastructure that respects user rights, ensures equitable access to technology and positively impacts overall well-being. Finally, by harnessing its convening capabilities, resources and political influence, the G20 can advocate for international cooperation around data regulation and governance. It can stimulate the formation of impactful and pragmatic global coalitions, guiding the alignment of national efforts with globally agreed best practices.

The most recent and consecutive presidencies of India, Brazil and South Africa in the G20 offer an unparalleled opportunity to advance the G20 digital agenda, especially for emerging economies. As influential states in the Global South, these BRICS nations can offer leadership that effectively bridges the digital divide while addressing the unique challenges of their respective regions and encouraging global cooperation.

Marking the culmination of the Indian presidency, the *G20 New Delhi Leaders' Declaration* articulated a set of priorities that promote the institution of "safe, secure, trusted, accountable and inclusive digital public infrastructure" and welcomed efforts to "build safety, security, resilience and trust in the digital economy". Moreover, it expressed a resolve to "foster safe and resilient digital ecosystems", to "build a comprehensive digital health ecosystem" in compliance with national data protection regulations, and to "promote responsible AI for achieving the Sustainable Development Goals (SDGs)", among other priorities.[6] The *Outcome Document* of the Digital Economy Minsters' Meeting, released earlier in August 2023, had addressed many of these themes as well, and also proposed strategies for digital skilling, and the introduction of upskilling and reskilling. It is expected that the Brazilian presidency might build further on some of these ideas and accelerators.

There is a unique opportunity to make critical technology recommendations and sustain these efforts across future presidencies, guiding global digital transformation and ensuring the sustainable, inclusive growth of the global digital economy. In essence, the G20's collective influence and diplomatic power make it a pivotal player in addressing shared global technology challenges and harnessing opportunities. Building on the impactful work led by the Indian presidency, this paper puts forward additional recommendations and considerations as consecutive G20 presidencies start to shape their G20 digital agendas.

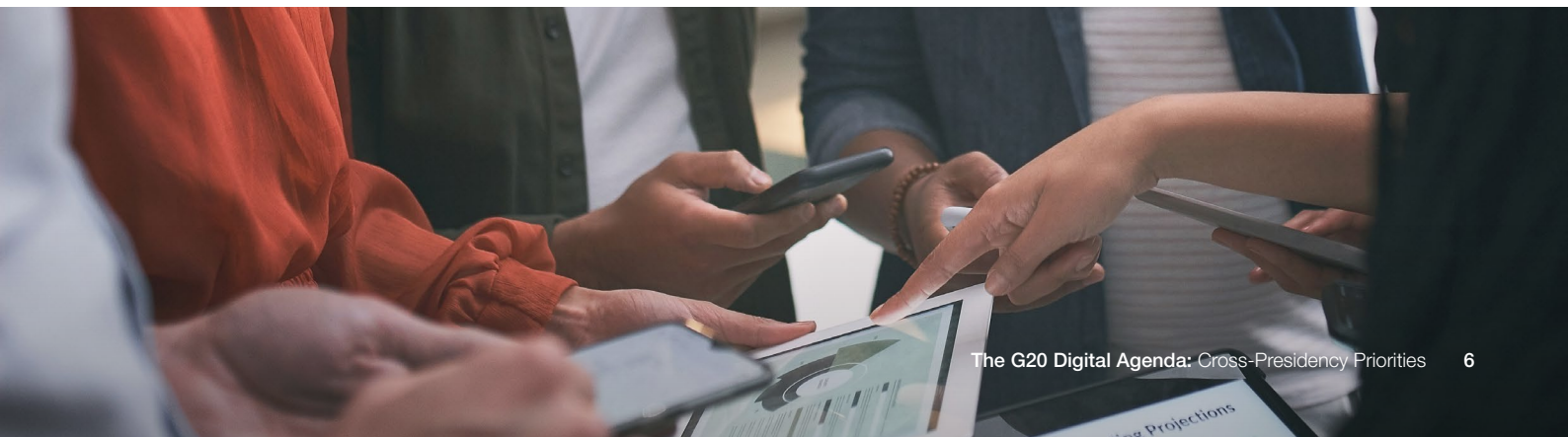
1 Focusing on the centrality of digital inclusion, access and trust

Cementing digital access, inclusion and trust are pivotal themes and fundamental to successfully invest and sustainably grow digital skills, public infrastructure, cybersecurity, health and sustainability.

To thrive in today's digitally connected world, people, organizations and governments need to access – and interact with – a trusted, global digital ecosystem. Economic trends suggest that technology stands as a key driver for a nation's economic expansion, linking directly to prosperity by enhancing the efficient production of goods and services.[8] Yet issues around digital access, trust, ownership, inclusion and security are becoming more complex, preventing all of society from fully benefiting from technological progress. Emerging technologies, such as quantum computing and artificial intelligence, have the potential to create significant economic and social benefits and address long-standing global challenges, including climate change and improving critical healthcare supply chains. Such technology is also a key source of competitive advantage for those with access to it; there is a growing and disproportionate rise in the power of those on the supply side of emerging technologies. While much of the algorithms and software are freely available, the digital industrial capacity to turn data into models at the multi-billion to trillion weight scale is an emerging barrier. Consequently, underrepresented groups must increasingly make the case that their language, culture and information should be included in these models.

These issues look different for every country. While some nations invest in pivotal social and economic pillars like skills, infrastructure, cybersecurity, health and sustainability, others formulate policies in these spheres, collaborate on technical standards and joint initiatives, or research to discern which actions catalyse, and which inhibit innovation and advancement. In this context, cementing digital access, inclusion and trust become pivotal themes and the core focus of this paper, especially within emerging economies. Emphasis leans towards women-led development, lowering barriers to entry for underrepresented groups (including women and small and medium enterprises) and promoting tech self-sufficiency of emerging market economies.

These themes are also the fundamental ingredients to successfully invest and sustainably grow digital skills, public infrastructure, cybersecurity, health and sustainability. Securing the G20's commitment to and support of these subjects could mark a pivotal moment for global progress. This relates to the G20's distinctive capacity, afforded by its extensive reach, to integrate nuanced regional diversities and local contexts when sculpting the future of technological solutions and assuring fair technology access. Consecutive G20 presidencies present a unique opportunity to address these issues collectively (with leadership from the Global South), driving these universal themes to ensure that digital access, inclusion and trust in emerging markets genuinely mirror global requirements and ambitions. In the context of these markets, issues of equity, inclusion and access among underrepresented communities and the technology domains explored in this paper are especially pronounced.



2

Ensuring cybersecurity of emerging technologies

In an interconnected world, cyberthreats pose a shared risk alongside the evolution of emerging technologies.

Ensuring the security of emerging technologies is vital to prevent an increase in global cybersecurity risks as they become more widespread.

Rapid digitization in the past few years has resulted in the growth of technology at a pace that is difficult for policy-makers and society to grasp. In response to digital transformation, emerging technologies and connected cybersecurity risks, many governments have started imposing cybersecurity requirements, especially when national security, economic security or public health and safety is at stake. The intentional design and implementation of these requirements need attention at the global policy level.

Digital and emerging technologies, ranging from the internet of things (IoT), generative artificial intelligence (AI) and quantum computing to advanced manufacturing, smart chemicals, artificial foods and human genome editing, can create tremendous social benefits. Yet they also create significant multi-dimensional risks. In an interconnected world, cyberthreats pose a shared risk alongside the evolution of emerging technologies, and since every part of the world has the potential to be connected, that shared risk is now a global risk.[9] As a result, cybersecurity policies and standards and the compliance or certification[10] against them must be globally interoperable across jurisdictions, with a baseline level of trust that extends across international boundaries. Therefore, the call for interoperability[11] across various local cybersecurity-related regulatory requirements is crucial for G20 countries and beyond.

Jurisdictional-specific cybersecurity regulatory requirements have increased substantially in the past few years. For example, in the last couple of years, Australia, China, India, the European Union, the United States and many others have enacted stringent cybersecurity regulatory requirements, referenced in this paper. These requirements are often based on or inspired by international standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[12] ISA/IEC 62443[13] and ISO/IEC 27000.[14] However, they are usually amended in some way,[15] diverging from what would have been common or interoperable international security requirements.

These jurisdictional-specific requirements pose several cybersecurity challenges. From a technical perspective, they may inadvertently leave out important cybersecurity controls or focus on specific technology solutions rather than broadly applicable principles. From a business perspective, jurisdictional-specific standards and certification requirements increase compliance burdens for manufacturers, service providers and cybersecurity professionals. This is especially the case when global products and international services must adhere to a multitude of requirements, translating to increased costs for customers. There are also compliance burdens for companies operating in multiple jurisdictions; in some cases, organizations may face mutually conflicting regulations, making full compliance and certification impossible.

Regulators may have good reason to include variations in their national standards to address local conditions. However, since the internet is globally interconnected, jurisdictional-specific regulations and certification requirements can easily become counterproductive. These local variations should be limited to the maximum extent possible to address specific conditions, and cybersecurity requirements should be common and interoperable across jurisdictions to every extent possible.

This problem is compounded further with respect to emerging technologies. Consensus-based and empirically tested “best practices” do not yet exist for many emerging technologies, such as generative AI or embedded biotechnology. The rapid development of such practices and standards for governance is urgently needed. Existing vulnerable information and operational technology already underpin most economic transactions, transport, healthcare, public services, supply chains and more, which creates enormous risks. These risks range from cybercrime’s economic impacts to public health and safety to geopolitical stability. Emerging technologies can amplify these risks by enhancing the capabilities of malicious actors and increasing reliance on digital solutions. Ensuring the security of emerging technologies is vital to prevent an increase in global cybersecurity risks as they become more widespread. Additionally, it is crucial to provide broad access to these technologies to ensure their benefits are widely distributed, not just concentrated among a few individuals or companies. To address these challenges, it is essential to proactively develop the capacity to manage key emerging technologies and address gaps in cybersecurity capabilities. Traditional regulatory tools may be insufficient and, in some cases, not applicable to enabling effective cybersecurity.

The G20 can play a crucial role in advocating for harmonized cybersecurity requirements that support both increased security and innovation. Many governments, including G20 governments, are working on this already and are considering, or have recently passed, policies to formulate cyber incident reporting regimes. Some examples are Australia's *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022*,[16] the EU's Network and Information Security 2 Directive and the US' *Cyber Incident Reporting for Critical Infrastructure Act*.[17] As these countries move towards implementation and as others contemplate similar cyber incident reporting policies, a critical moment emerges for interoperability across such policies. Interoperability can be established based on adherence to jurisdictional-specific policies with industry best practices, such as the European Union Agency for Cybersecurity (ENISA) *Good Practice Guide on Incident Reporting*,[18] the National Institute of Standards and Technology (NIST) *Incident Handling Guide*,[19] and the Cyber Threat Alliance *Cyber Incident Reporting Framework*.[20]

Given the risk that cybersecurity poses in the context of digital and emerging technologies, the G20 Digital Agenda should incorporate cybersecurity technologies as a key focus area across consecutive presidencies. This paper advocates for the G20 to undertake the following actions:

- Support the development and mutual recognition of voluntary cybersecurity certification for devices, service providers and professionals, building on the Common Criteria platform, which includes basic device certification. Certification could be developed in collaboration with standards development organizations (Institute of Electrical and Electronics Engineers Standards Association, International Standards Organisation, European Telecommunications Standards Institute, European Committee for Standardization, Connectivity Standards Alliance[21]), with a goal of agreeing on the minimum requirements for certifications across different domains.

- As jurisdictions continue to develop and implement cybersecurity policies, the G20 should facilitate the creation of international ontological standards.[22,23] These standards should contain concepts, definitions and axioms to formally represent what constitutes a reportable incident, when, how and to whom reporting is required, and what baseline level of security is required, among other aspects. The G20 can support this by working with its international partners to establish commonalities and define the baseline level of trust to minimize jurisdictional-specific requirements.

- Recognizing both the benefits and potential costs of AI technology, the G20 should endorse the formation of AI security practices for countering global threats, promote the use of these best practices, identify potential governance mechanisms and develop proofs-of-concept for accountability.

3

Investing in digital health and sustainability solutions

The G20, with its unique position, can significantly impact and drive investment towards global health and sustainability challenges as they become increasingly interconnected.

Individuals, companies, communities and governments will only continue to adopt sustainable solutions if they trust them and fully understand their benefits.

The challenges of digital health and sustainable solutions transcend borders and geopolitical lines. Both health and environmental sustainability are vital components of any digital agenda, as they are interconnected. Climate change poses health risks, including storm injuries, infectious diseases and chronic illnesses, disrupting healthcare and food security. In addition, extreme weather events, gradual warming and changes in humidity indirectly affect human health by disrupting healthcare delivery and endangering food security. Vulnerable populations, even in high-income countries, are disproportionately affected, exacerbating health disparities. [24]

During the COVID-19 pandemic, digital technology and data flows enabled several critical responses, including data sharing for medical research and response, monitoring and controlling vaccine production and distribution, and adopting digital services for business and public service to prevent disruption.[25] During the pandemic, several platforms emerged that collected data from around the world to track and assess these trends.[26] These efforts paved the way for several pioneering cross-border data health initiatives. Similarly, digital technologies hold significant promise for sustainable development.[27] They are already being deployed to address a range of sustainability challenges,[28] from climate change to the monitoring of wildfires to mapping and protecting biodiversity.

Global investment in digital health and sustainability showcases innovation in these areas. Early-stage funding and mega-deals indicate the transformation of healthcare through emerging technologies. Despite this, overall global digital health investment is at its lowest since 2017. [29]

Beyond electrification and renewables, critical areas of investment and opportunity include carbon capture and storage, carbon removal technologies, circular technologies, sustainable agriculture and water and biodiversity solutions. These areas will require deep private and public partnerships, new foresight methods to illuminate what comes next and systems-level approaches. G20 countries are well-positioned to lead the charge in developing all of these.

Inclusion, access and trust are essential for successful emerging technology innovation in digital health and sustainability solutions. Policy-makers, industry leaders and healthcare systems must address critical challenges, including AI and machine learning, innovations in electronic health records, gene editing and precision medicine at large, and data privacy and security.[30] Securing personal data is crucial to build confidence in these technologies. Global stakeholders must continue to consider and innovate around data privacy and security to ensure scalability and adoption by both patients and medical professionals.[31] The World Economic Forum's Centre for Health and Healthcare collaborates with the G20 to drive data-driven health initiatives, aiming to address global healthcare challenges, including equitable access to care and improved health outcomes through public-private partnerships.

There is a similar interconnectedness between access, inclusion and trust and the growth of emerging technologies in sustainable development solutions. Transitioning to sustainable solutions, such as electric cars and efficient smart home technologies, comes with costs, posing the risk that only those who can afford them will access these emerging technologies. Further, individuals, companies, communities and governments will only continue to adopt sustainable solutions if they trust them and fully understand their benefits. The G20 can play an active and invaluable role in ensuring precision data security and minimizing precision data bias and underrepresentation, thereby improving overall digital trust in both the digital health and sustainability spheres.

Ease of use, linked to digital literacy, continues to pose a critical challenge, with electronic patient records, for example, facing adoption headwinds due to design principles that seemingly lack user-centricity.[32] Other challenges include maintaining an ability to adapt to evolving patient needs, as well as determining the right, trusted and patient-accepted role for AI in the broader digital health ecosystem.[33] Addressing these challenges demands multistakeholder and global partnerships and will

require private investment and innovation, public regulation and cross-border cooperative frameworks, as well as changes in individual behaviour.

The G20, with its unique position, can significantly impact global health and sustainability challenges as they become increasingly interconnected. G20 countries possess substantial innovation funding sources,[34] exemplified by $120 billion in investments in nature-based solutions in 2020, representing 92% of global spending in this area. Further, the spending gap in non-G20 countries is larger and more difficult to bridge than in G20 countries,[35] demonstrating the capacity of G20 countries to drive investment towards digital health and sustainability solutions. To meet agreed biodiversity, land restoration and climate targets by 2050, G20 annual investments in nature-based solutions must increase by 140%, requiring an extra $165 billion yearly, mainly in Official Development Assistance (ODA) and private-sector spending.

This paper recommends that the G20 support:

- **Driving greater G20 investment in digital health and sustainability solutions from G20 countries:** The G20, with its substantial size and influence, can establish mechanisms to propel global investment in digital health and sustainability solutions. This may involve creating incentives for private sector investment in their countries and supporting innovative, early-stage companies tackling challenges in these domains.
- **Endorsing AI standards in digital health and sustainability:** AI is poised to play a significant role in healthcare and sustainability.[36] The G20 can lead efforts to define AI's role, identify gaps and set clear agendas.[37] This includes enhancing sectors like supply chains, logistics, design, energy efficiency, agriculture and disaster preparedness. Additionally, the G20 can promote standards to reduce bias and improve inclusivity in AI-enabled solutions.
- **The continuation of a commitment to using data for sustainable development:** G20 countries can build on previous efforts announced in Bali,[38] developing frameworks for open repositories. These frameworks facilitate sharing national health and sustainability datasets, harmonizing data standards, improving data portability and enhancing system interoperability. They can also strengthen mechanisms for transnational data sharing during global health and sustainability crises.

4

Enabling digital infrastructure

The G20 is well-positioned to create a conducive environment for cross-border data flows and digital public infrastructure, thereby driving global digital economic growth.

To harness the economic potential of digitization, societies need inclusive and collaborative digital and physical infrastructure.

The global digital revolution has made data a crucial resource for innovation, economic growth and societal progress. Data is at the centre of governance discussions due to its socioeconomic significance and its potential to address global challenges. However, data use can either create collaboration or exacerbate inequalities across borders. Effective standardized frameworks for data collection, decoding, storage and use are essential for successful governance of emerging technologies.

Data is a critical component and needs to be understood as a key part of modern-day infrastructure. It also presents new challenges to existing institutions concerned with the safe and effective management of infrastructure. Having a strong understanding of "data as infrastructure" and the need to develop holistic "data infrastructure" will only become more vital as populations grow and economies and societies become increasingly reliant on getting value from data to meet people's needs and deliver on global ambitions, including the Sustainable Development Agenda.

Even within the G20, the data ecosystem is neither uniform nor unified – the same information about an entity in the environment has different representations and, consequently, different meanings. Diverse information and representations hinder interoperability, limiting international cooperation. Regulatory challenges arise due to the sensitivity of information, especially concerning the needs and priorities of sovereign nations.

In a rapidly advancing digital age, the free flow of data across borders is essential for innovation, economic growth, social progress and transformative change. Achieving this will require that data is harnessed in interoperable rather than fragmented national infrastructures. Cross-border data flows (CBDFs) offer opportunities for global collaboration, economic growth and scalable solutions to challenges like climate change. Discussions on this topic are influenced by tensions around free trade, privacy and data protection. Misuse and data quality issues can exacerbate conflict. Trust is crucial for CBDFs, requiring dedicated frameworks. Data Free Flow with Trust (DFFT) has been a key agenda item for the G7 and G20, supported by several international organizations, including the World Economic Forum and the Organisation for Economic Co-operation and Development (OECD).[39] Differing regulations, privacy, ethics and digital disparities remain challenges to CBDFs.

Access, inclusion and trust are central to discussions on increased investment in digital infrastructure. To harness the economic potential of digitization, societies need inclusive and collaborative digital and physical infrastructure. One such mechanism is the evolution of digital public infrastructure (DPI), an ecosystem-wide approach focusing on universal access, interoperability and innovation. This is often designated as a "stack", which is a common concept in software development consisting of "a set of components working together effectively and efficiently to execute an application and for data to flow".[40] DPI is an approach that creates societal outcomes within and across sectors by building open and interoperability technology building blocks, along with transparent, accountable and participatory governance frameworks and enabling public, private and civil DPI creates societal benefits through open technology building blocks, transparent governance and partnerships across sectors. For instance, India's Unified Payments Interface connects millions of banks and merchants, expanding financial access.[41] Similarly, in education in India, Digital Infrastructure for Knowledge Sharing (DIKSHA) provides millions of teachers and students with locally-created content.[42]

Amid rapid technological progress, investing in DPI is essential for global development. The recent Indian G20 presidency recognized this as a key priority. DPI ensures inclusive digital access, transparency and interoperability, akin to vital public services. Brazil's PIX, for example, has enabled financial payments across the country.[43] The United Arab Emirates invested in a unified digital identity platform, UAEPass, which allows both residents and visitors to access and perform many government and private sector services and to sign formal documentation digitally.[44] The platform was used for the 2023 Federal National Council elections process in the country, enabling voters to cast their votes from anywhere without visiting polling stations.[45]

The scaling of DPI solutions relies on trusted data exchanges, both within countries and across borders. Simultaneously, DPI serves as a critical building block for these data flows, enabling efficient and equitable public services that span geographical boundaries. DPI not only addresses various development needs but also gives governments more control over their technology foundations and data. This control is especially evident when governments implement policies related to antitrust, interoperability standards and data protection. As such, DPI is intrinsically linked to data flows, and, when designed, manufactured and operated with inclusion and local capacity in mind, DPI can unlock a range of lasting socioeconomic solutions.

Challenges in using CBDFs for DPI intersect technology, policy and geopolitics. Growing data sharing raises privacy concerns, potentially hindering cross-border data access. Cybersecurity threats like breaches and attacks jeopardize DPI's confidentiality, integrity and availability. Diverse data standards, structures and regulations across jurisdictions complicate global DPI development. Issues such as digital sovereignty, power imbalances and North-South disparities could impede DPI's effectiveness. Political instability, conflicts and corruption divert resources from digital infrastructure, exacerbating access disparities.

The G20 is well-positioned to address these challenges, which are critical to creating a conducive environment for CBDFs and DPI, thereby driving global digital economic growth. This paper recommends that the G20 support:

- **Development of global data governance standards:** The G20, through its Digital Economy Working Group,[46] should lead efforts to create a widely-accepted set of data governance standards. These standards should encompass data privacy, ethical use, cybersecurity and interoperability, allowing for effective and responsible CBDFs and building on previous ministerial meetings. There should be a discerning and judicious balance between ensuring the legitimate use of data for innovation and business growth while also respecting the need for data security and data privacy. This effort must connect to and complement the work of other multilateral fora, including the G7 and United Nations Global Digital Compact.

- **Support the design of frameworks:** The G20 can support the design of robust and adaptable frameworks implemented in settings that can enable innovations (e.g. cross-border sandboxes) to provide the necessary safeguards for countries while still enabling innovation.

- **Global data cooperation:** The G20 should encourage global multistakeholder coalitions centred around ontological data (e.g. *IEEE 1872-2015 Standard Ontologies for Robotics and Automation* and *IEEE 7007-2021 Ontological Standard for Ethically Driven Robotics and Automation Systems*) to facilitate a clear and unambiguous dialogue among different stakeholders and to enable system's interoperability. It can encourage countries, businesses and other data-deploying organizations to share best practices and common issues, align national efforts with global guidelines, regulations and standards, and collaborate on innovative solutions.

5

Building digital skills

The new kinds of jobs emerging in the global digital economy will require different skills to work more closely with intelligent machines, data and algorithms.

The disruptive transformation of the digital age comes from the adoption and application of new technologies – changing not just what governments and organizations across sectors do but also how they operate. Digital skills are the foundation of these changes, providing individuals – as workers in enterprises and citizens across cultures – with the knowledge and expertise to contribute meaningfully to digitalization. In this sense, such skills have become the lifeblood of socioeconomic resilience and societal digital transformation. In order to meet this ambition, governments need these digital skills as well. Public agencies and their constituent staff need to have the capacity to regulate, use and enable technologies to steer societies towards a safer, more prosperous and more sustainable digital future.

Digital skilling and upskilling are intertwined with digital inclusion, access and trust and are critical to bridging the digital divide. Central to this is a recognition of alternative pathways to careers by investing in educational programmes that provide in-demand skills at scale, including "earn and learn" programmes like apprenticeships, new hybrid education models, partnerships between communities, technical and/or vocational colleges and the private sector, among others. Digital capability building is necessary not only for citizens but also for regulators. Countries must commit to modernizing their education systems to meet the demands of the digital economy. In this regard, ensuring access to research, academic and start-up communities helps ensure access to broader groups of innovators, especially those in underrepresented groups. Additionally, as the global build-out of public digital infrastructure (PDI) progresses, there is a need for coordinated strategies to ensure local involvement in its design, manufacturing, deployment and support. This approach offers a chance to enhance IT and operational technology (OT) expertise, bolstering both innovation in the global academic and research community and competitiveness in the technology marketplace.

The "reskilling revolution" is now unfolding, marking the onset of a transformative era.[47] The new kinds of jobs emerging in the global digital economy will require different sets of skills to work more closely with intelligent machines, data and algorithms. The World Economic Forum's *Future of Jobs Report 2023* predicts that 23% of global jobs will change in the next five years due to industry transformation, including through AI and other text, image and voice processing technologies.

Employers foresee that within a five-year timeframe, approximately 44% of workers' skill sets will experience transformation. During this same period, technology literacy is identified as the third most swiftly evolving core skill. This highlights the escalating importance of digital skills and the ability to use them adeptly.[48]

According to data from LinkedIn, the roles with the fastest growth rates include AI Specialist, Robotics Engineer, Data Scientist and Developer.[49] Each of these roles requires a strong set of technical skills, from a close understanding of data to a familiarity with working with the latest cutting-edge technology. An understanding of digital technologies, particularly AI, however, will increasingly become a prerequisite for both those looking to enter the workforce and those with already established careers. The digital maturity across nations necessitates a holistic and inclusive approach to digital skills.

Building digital skills presents a number of challenges that are related to the capabilities of individuals, regulation and technological infrastructure. For instance, these may include differences in individual ability, level of instructors, socio-digital inequities, students' economic conditions, a lack of government initiatives and a weak technological environment. Furthermore, modifying curricula is typically a very sluggish process that requires lengthy procedures, the creation of several committees and the provision of funding for high-level decision-making. The G20 has already made an investment in creating a roadmap for assessing digital skills literacy per country.[50] More efforts can be made to build upon this tool. While challenges exist in building digital skills, the opportunities they offer in terms of employability, career growth, entrepreneurship, global reach, innovation and personal development are substantial. Embracing and developing digital skills can lead to a more dynamic and fulfilling personal and professional life in today's digital age.

“ Rapid digital transformation in recent years has resulted in a global phenomenon of digital skills shortage in almost every industry.

Even in those G20 countries where the challenges of faculty, curriculum and incentives are tractable, one distinct characteristic of many of the emerging technologies is the scale of infrastructure required to gain proficiency and to contribute to the supply side of the digital economy. For instance, training a single AI model may consume enormous amounts of energy and occupy a massive computational cluster for months, yielding considerable operational costs on top of the capital costs of the high-performance compute, network and storage infrastructure. These challenges hinder the development of expertise in current advanced techniques. This leads to immediate labour shortages and specialized skill demands, which only a few enterprises with sufficient capital and operational resources can address.

When advancements are tied solely to the ongoing production supply chain, academics, researchers and start-ups are less likely to introduce novel materials and processes for fear of compromising critical production. As G20 members look towards large-scale public/private infrastructure investments, there is an opportunity to incorporate negotiated access and support for (beyond) state-of-the-art training and experimental capacities, like global opportunities provided by the MOSIS Service over the past four decades. In the AI space, proposals such as the US National AI Research Resource could serve as models for offering not only data and computational resources to underrepresented research groups but also opportunities for these communities to engage with ethical and responsible design practices.

The pervasive build-out of PDI itself also provides a unique opportunity for G20 members, who have traditionally focused investment on skill development built upon lower-level technologies, to expand their participation in the supply side. In prior generations of technological adoption, technicians, engineers and entrepreneurs each played roles, successively deepening supply chain involvement. This progression promoted innovation, competition and broadened access by tailoring to local languages and cultures. This can only happen now, however, if there is direct engagement with nascent academic and workforce reskilling communities in the design, manufacturing, deployment and maintenance of PDI. Outsourcing PDI to in-country but remotely designed and managed “black-box” solutions might be cost-effective, time-efficient and address data sovereignty issues. However, this approach can restrict long-term economic growth, perpetuate supply concerns and widen the digital divide between underrepresented groups and their own PDI.

The fast pace of emerging technologies, including AI, however, poses significant challenges. Rapid digital transformation in recent years has resulted in a global phenomenon of digital skills shortage in almost every industry.[51] There is a general need for regulatory capability-building in IT and OT for both technology consumers and technology producers. As the world becomes increasingly connected, cyber-physical effects become more pronounced and widespread; therefore, IT and OT knowledge will become increasingly pertinent for both cybersecurity professionals and regulators. This demonstrates a need to accelerate digital capacity building for regulators, technology producers and consumers alike. The challenges to digital upskilling for technology consumers or citizens are equally relevant. Infrastructure challenges, budget constraints and language barriers are notable barriers, to name a few.

Although efforts to bridge the digital skills gap have been ongoing, IT/OT professionals are still in high demand. Despite few schools currently offering OT training programmes, there have been recent government-supported programmes offered in

some countries such as Israel[52] and Singapore,[53] and in cybersecurity-focused institutions like the SANS Institute. The G20 can help enable the right conditions and frameworks for the sharing of industry expertise with regulators to equip the stewards of the digital revolution with the necessary and relevant skills. The US recently released the *National Cyber Workforce and Education Strategy*, a comprehensive strategy to address cyber workforce needs.[54] A similar approach can be adopted for capacity building at the G20 level across different emerging technology domains. In parallel, different skilling competency frameworks have been developed in the EU[55] and other countries, including Singapore,[56] and an internationally recognized framework called Skills Framework for the Information Age (SFIA) has been adopted by some countries. Moreover, countries and cities like the UK[57] and Dubai[58] started introducing new certification requirements for digital professionals based on those frameworks. Therefore, such frameworks can serve as a foundation for global digital skills certification efforts.

The G20 should support:

- **A G20 digital skills and literacy initiative for regulators:** This initiative would focus on the development and dissemination of digital skills and literacy programmes for regulators across member countries. Building on existing efforts, including the G20's commitment to an interconnected digital economy, the initiative can work towards creating standard guidelines for digital education and literacy, adapting to the specific needs of different regulators.
- **The creation of a G20 digital infrastructure investment fund for regulatory capability building:** Through the G20's Infrastructure Working Group's efforts to improve infrastructure globally, this fund can specifically target digital infrastructure and resources needed to support digital skills development for regulators, technology consumers and technology producers, making emerging technologies, cybersecurity, IT and OT education and upskilling programmes more accessible to policy-makers worldwide.
- **Establishment of an engagement group for digital skills global certification:** Such a group could be based on a mutually recognized competency framework that allows G20 countries to acknowledge each other's requirements and qualifications and, therefore, enables professionals to offer their services in different countries without global restrictions. An example is the *Operational Technology Cybersecurity Competency Framework*[59] developed by Singapore's Cyber Security Agency and Infocomm Media Development Authority in consultation with industry and academia – which the US Cybersecurity and Infrastructure Security Agency has taken note of.[60] The framework can be regularly reviewed and updated with each consecutive presidency to keep pace with a changing digital landscape. Such an engagement group could also support the establishment of an international board for certifying digital specialists, similar to medicine and engineering international boards.

Conclusion

The most recent and consecutive presidencies of India, Brazil and South Africa, respectively, in the G20 offer an unparalleled opportunity to advance the G20 digital agenda, especially for emerging economies. Each of these countries is a significant player in the Global South, and together, they can offer leadership that effectively bridges the digital divide, simultaneously addressing the unique challenges of their respective regions and promoting global cooperation.

India, with its burgeoning digital economy and experience in building extensive digital public infrastructures for use at scale, has already paved the way for the G20's digital agenda on sharing best practices and collaboratively creating global data governance standards that influence multiple sectors. Using its Aadhaar project experience, India has shared valuable insights on implementing a large-scale digital infrastructure while addressing concerns of data privacy and security.

Brazil, with its robust digital sector and its experience in e-governance, can champion the cause of digital inclusivity. Brazil's presidency can focus on ensuring that the benefits of digital transformation are equitably shared, drawing on its own efforts to increase digital access across its vast and diverse territory.

South Africa, as a continental leader in Africa, can underline the need for global digital cooperation. By sharing its experiences navigating the digital economy's challenges and opportunities, South Africa can help the G20 promote global partnerships and encourage countries to align their national efforts with global best practices.

Consecutive presidencies form a coherent trajectory, building upon each other's work and sustaining momentum on the G20 digital agenda, ensuring a more inclusive and equitable digital future for all.

Contributors

Working Group on G20 Digital Agenda

Bushra AlBlooshi
Head, Research and Innovation,
Dubai Electronic Security Center

Miguel Amaral
Senior Policy Analyst,
Organisation for Economic Co-operation
and Development (OECD)

Marta Arsovska Tomovska
Director, Digital, Office of the
Prime Minister of Serbia

Fatmah Baothman
Associate Professor in AI,
King Abdulaziz University

Linda Bonyo
Founder, Lawyers Hub

Kirk Bresniker
Fellow, Vice-President and
Chief Architect, Hewlett Packard Labs,
Hewlett Packard Enterprise

Michael Daniel
President and Chief Executive Officer,
Cyber Threat Alliance

Roslyn Docktor
Vice-President, Technology
and Science Policy, IBM

Aaron Maniam
Researcher, Blavatnik School
of Government, University of Oxford

Robb Henzi
Partner and Head, Policy and Philanthropy
Practice, sparks & honey

Yurie Ito
Founder and Executive Director,
CyberGreen Institute

Astha Kapoor
Co-Founder, Aapti Institute

Hoda Al Khzaimi
Director, Centre for Cybersecurity

Paul Klimos
Senior Associate, Orrick

Nele Leosk
Ambassador-at-Large,
Ministry of Foreign Affairs of Estonia

Lindiwe Matlali
Chief Executive Officer, Africa Teen Geeks

Charmaine Ng
Director, Digital Policy,
Asia Pacific, Schneider Electric

Edson Prestes
Full Professor, Federal University
of Rio Grande do Sul

Carolina Rossini
Co-Founder and Director,
Policy and Research,
The Datasphere Initiative Foundation

Samir Saran
President, Observer
Research Foundation (ORF)

Vikram Sharma
Founder and Chief Executive Officer,
QuintessenceLabs

Vera Songwe
Nonresident Senior Fellow,
Brookings Institution

Ning Wang
Research Group Leader,
University of Zurich

Xue Lan
Professor; Dean, Schwarzman College
Tsinghua University

World Economic Forum

Priya Vithani
Engagement Lead, Centre for the
Fourth Industrial Revolution

Acknowledgements

Sebastian Buckup
Member of Executive Committee,
World Economic Forum

Ariel Kastner
Head, Geopolitical Agenda
and Communications,
World Economic Forum

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Martha Howlett
Editor, Studio Miko

Endnotes

1. Jain, Shruti, *The G20 Digital Economy Agenda for India*, Observer Research Foundation (ORF) Online, 2022, https://www.orfonline.org/research/the-g20-digital-economy-agenda-for-india/.
2. "What is the G20?", *Organisation for Economic Co-operation and Development (OECD)*, n.d., https://www.oecd.org/g20/about/.
3. United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2021*, 2021, https://unctad.org/page/digital-economy-report-2021.
4. "Ministers Responsible for the Digital Economy", *G20 Research Group*, 19 August 2023, http://www.g20.utoronto.ca/digital/index.html.
5. World Economic Forum, *Shaping a Multiconceptual World*, 2020, https://www3.weforum.org/docs/WEF_Shaping_a_Multiconceptual_World_2020.pdf.
6. G20 2023 India, *G20 New Leaders' Declaration*, 2023, https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf.
7. G20 2023 India, *Digital Economy Ministers Meeting: Outcome Document & Chair's Summary*, 2023, https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20_Digital_Economy_Outcome_Document%20_and_Chair%27s_Summary_19082023.pdf.
8. Hausmann, Ricardo and José Domínguez, "Knowledge, Technology and Complexity in Economic Growth", *Harvard University*, n.d., https://rcc.harvard.edu/knowledge-technology-and-complexity-economic-growth.
9. World Economic Forum, *The Global Risks Report 2023*, 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.
10. Cybersecurity certification has extended beyond devices and includes professional and service provider certifications as well.
11. World Economic Forum, *International Cybersecurity Certification Framework: Pathways to Collaboration and Situational Analysis*, 2021, https://www3.weforum.org/docs/WEF_GFC_Cybersecurity_International_Certification_Framework_2021.pdf.
12. "Cybersecurity Framework", *National Institute of Standards and Technology (NIST)*, n.d., https://www.nist.gov/cyberframework.
13. "ISA/IEC 62443 Series of Standards", *International Society of Automation*, n.d., https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
14. "ISO/IEC 27000 family", *International Organization for Standardization (ISO),* n.d.,https://www.iso.org/standard/iso-iec-27000-family.
15. "Revealing New Opportunities for the Cybersecurity Workforce", *ISC2*, n.d., https://www.isc2.org/Research/rusi-rehttps://blog.isc2.org/isc2_blog/2023/04/rusi-and-isc2-report-rapid-evolution-of-cybersecurity-policy-raises-need-for-cross-border-standardiz.html.
16. "Security Legislation Amendment (Critical Infrastructure Protection) Act 2022", *Australian Government Department of Home Affairs*, n.d., https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022.
17. US Senate Committee on Homeland Security & Governmental Affairs, *Cyber Incident Reporting for Critical Infrastructure Act*, 2021, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Overview%20of%20Cyber%20Incident%20Reporting%20Legislation.pdf.
18. European Union Agency for Cybersecurity (ENISA), *Good Practice Guide on Incident Reporting*, 2009, https://www.enisa.europa.eu/topics/incident-reporting/for-telcos/guidelines/good-practice-guide-on-incident-reporting.
19. NIST, *Computer Security Incident Handling Guide*, 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
20. Cyber Threat Alliance, *Cyber Incident Reporting Framework*, 2022, https://www.cyberthreatalliance.org/resources/assets/cyber-incident-reporting-framework/.
21. "The New United States Cybersecurity Label Drives Forward the IoT", *Connectivity Standards Alliance*, 18 July 2023, https://csa-iot.org/newsroom/the-new-united-states-cybersecurity-label-drives-forward-the-iot/?utm_campaign=Member%20and%20Interest%20List%202023&utm_content=2572s05884&utm_medium=social&utm_source=linkedin&hss_channel=lcp-1922026.
22. Prestes, Edson, Michael A. Houghtaling, Paulo J.S Gonçalves, Nicola Fabiana et al., "The First Global Ontological Standard for Ethically Driven Robotics and Automation Systems", *Institute of Electrical and Electronics Engineers (IEEE) Robotics & Automation Magazine*, December 2021, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9646310.
23. "IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems", *IEEE Standards Association*, n.d., https://standards.ieee.org/ieee/7007/7070/.
24. "Sustainability and Health", *McKinsey Health Institute*, n.d., https://www.mckinsey.com/mhi/focus-areas/sustainability-and-health.

25. "COVID-19 Dashboard", *John Hopkins University*, n.d., https://coronavirus.jhu.edu/map.html.
26. Vithani, Priya, Arushi Goel and Fumiko Kudo, *Building Bridges: Aligning Digital Public Infrastructure and Cross-Border Data Flows*, ORF Online, 2023, https://www.orfonline.org/research/building-bridges/#_edn34
27. "Digital technologies to achieve the UN SDGs", *International Telecommunication Union (ITU)*, December 2021, https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx.
28. "3 ways technology is helping the world adapt to climate change", *World Economic Forum*, 1 February 2023, https://www.weforum.org/agenda/2023/02/technology-climate-change-adaptation/.
29. CB Insights, *State of Digital Health Q2'23 Report*, 2023, https://app.cbinsights.com/research/report/digital-health-trends-q2-2023/.
30. Brodwin, Erin and Tina Reed, "Privacy is at risk as HIPAA fails to keep pace with digital health", *AXIOS*, 6 April 2023, https://www.axios.com/2023/04/06/privacy-risk-hipaa-digital-health.
31. Nabholz, Christoph, "Trust: the foundation of our digital health care transition", *Swiss RE Group*, 29 June 2023, https://www.swissre.com/institute/research/topics-and-risk-dialogues/health-and-longevity/foundation-of-digital-health-care-transition.html.
32. Betton, Victoria, "EPR Adoption — Is User-centred Design the Key to Usability?", *The Journal of mHealth*, 7 December 2022, https://thejournalofmhealth.com/epr-adoption-is-user-centred-design-the-key-to-usability/.
33. Vigario, Paul, "2023: The Year to Focus on Creating a Better Patient Experience", *The Journal of mHealth*, 4 January 2023, https://thejournalofmhealth.com/2023-the-year-to-focus-on-creating-a-better-patient-experience/.
34. "G20 Countries Can Help Close Climate Finance Gap by Investing in Nature-based Solutions", *World Economic Forum*, 26 January 2022, https://www.weforum.org/press/2022/01/g20-countries-can-help-close-climate-finance-gap-by-investing-in-nature-based-solutions/.
35. United Nations Environment Programme (UNEP), *The State of Finance for Nature in the G20 report*, 2022, https://www.unep.org/resources/report/state-finance-nature-g20-report.
36. Bishen, Shyam, "World Health Day: Here's how AI and digital health are shaping the future of healthcare", *World Economic Forum*, 6 April 2023, https://www.weforum.org/agenda/2023/04/world-health-day-how-ai-and-digital-health-healthcare/.
37. Mandaviya, Mansukh, "G20 offers rare chance to forge global vision for digital health", *Business Live*, 16 May 2023, https://www.g20.org/content/dam/gtwenty/gtwenty_new/press-spotlight/MANSUKH_MANDAVIYA_%20G20.pdf.
38. "Data for Development: Role of G20 in Advancing the 2030 Agenda", *ORF Online*, 3 Janaury 2023, https://www.orfonline.org/research/data-for-development/.
39. "Moving forward on data free flow with trust: New evidence and analysis of business experiences", *OECD*, 2023, https://www.oecd-ilibrary.org/science-and-technology/moving-forward-on-data-free-flow-with-trust_1afab147-en.
40. Identification for Development (ID4D), *A Digital Stack for Transforming Service Delivery: ID Payments, and Data Sharing*, 2022, https://documents1.worldbank.org/curated/en/099755004072288910/pdf/P1715920edb5990d60b83e037f756213782.pdf.
41. Abraham, Sunil, *Unified Payment Interface: Towards Greater Cyber Sovereignty*, 2020, https://www.orfonline.org/research/unified-payment-interface/.
42. Alonso, Cristian, Tanuj Bhojwani, Emine Hanedar, Dinar Prihardini et al., "Stacking up the Benefits: Lessons from India's Digital Journey", *International Monetary Fund (IMF) Working Papers*, vol. 2023, issue 78, 31 March 2023, https://www.elibrary.imf.org/view/journals/001/2023/078/article-A001-en.xml.
43. Cook, William, "Comparing India's UPI and Brazil's New Instant Payment System, PIX", *Consultative Group to Assist the Poor (CGAP)*, 2 February 2021, https://www.cgap.org/blog/comparing-indias-upi-and-brazils-new-instant-payment-system-pix.
44. "The UAE Pass app", *The United Arab Emirates' Government*, 23 May 2023, https://u.ae/en/about-the-uae/digital-uae/digital-transformation/platforms-and-apps/the-uae-pass-app.
45. "NEC adopts executive regulations of 2023 FNC elections", *Emirates News Agency-WAM*, 6 July 2023, https://www.wam.ae/en/details/1395303175175.
46. "Sherpa Track", *G20 2023 India*, n.d., https://www.g20.org/en/workstreams/sherpa-track/.
47. "The Reskilling Revolution", *World Economic Forum*, n.d., https://initiatives.weforum.org/reskilling-revolution/home.
48. World Economic Forum, *Future of Jobs Report 2023, 2023,* https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.
49. LinkedIn, *2020 Emerging Jobs Report*, 2020, https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/emerging-jobs-report/Emerging_Jobs_Report_U.S._FINAL.pdf.
50. CSIS Indonesia, *G20 Toolkit for Measuring Digital Skills and Digital Literacy: Framework and Approach*, 2022, https://s3-csis-web.s3.ap-southeast-1.amazonaws.com/doc/Digital_Skills_Toolkit_Final_Report_FINAL_Part_I.pdf?download=1.
51. RAND, *The global digital skills gap*, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1533-1/RAND_RRA1533-1.pdf.

52. Blassiau, Christophe, “Public-Private Collaboration on Display at Israel Cyber Week”, *US Chamber of Commerce*, 31 August 2022, https://www.uschamber.com/security/cybersecurity/public-private-collaboration-on-display-at-israel-cyber-week.

53. Cyber Security Agency Singapore, *Operational Technology (OT) Cybersecurity Competency Framework*, 2021, https://www.csa.gov.sg/docs/default-source/csa/documents/publications/otccf/ot-cybersecurity-competency-framework_v5.pdf?sfvrsn=edc6809a_0.

54. “FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America’s Cyber Talent”, *The White House*, 31 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/.

55. “DigComp”, *European Commission*, n.d., https://joint-research-centre.ec.europa.eu/digcomp_en.

56. “Skills Framework for Infocomm Technology (SFw for ICT)”, *Infocomm Media Development Authority*, n.d., https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/skills-framework-for-infocomm-technology-sfw-for-ict.

57. “NCSC Certified Cyber Professional (CCP) assured service”, *British Computer Society*, n.d., https://www.bcs.org/qualifications-and-certifications/certifications-for-professionals/inform ation-security-and-ccp-assured-service-certifications/ncsc-certified-cyber-professional-ccp-assured-service/.

58. “Cyber Force”, *Dubai Cyber Innovation Park*, n.d., https://dcipark.gov.ae/cyber_force/.

59. Cyber Security Agency Singapore, *Operational Technology (OT) Cybersecurity Competency Framework*, 2021, https://www.csa.gov.sg/docs/default-source/csa/documents/publications/otccf/ot-cybersecurity-competency-framework_v5.pdf?sfvrsn=edc6809a_0.

60. Cyber Security Agency of Singapore, *Operational Technology Cybersecurity Competency Framework (OTCCF)*, 2021, https://www.csa.gov.sg/Tips-Resource/publications/2021/operational-technology-cybersecurity-competency-framework-(otccf).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org