GLOBAL SOLUTIONS
THE WORLD POLICY FORUM

ISSUE 9

GLOBAL SOLUTIONS JOURNAL

RECOUPLING

THE GLOBAL SOLUTIONS SUMMIT 2023 EDITION

AKINSEMOLU • ALBRIEU • ANBUMOZHI • BARROS • BERGER • BERMONT DIAZ
BOIX • BRADFORD • CARVALHO • CHADHA • CHARVET • DROSTE • ELVERDIN
ENGELS • EULER • GARCIA VILLAMIL • GONCALVES • GÖRLICH • GOVENDER
GRAINGER • GREENLAND • GUPTA • HAUT • HEINKE • HIRAWAN • HYUN
JOOSTEN • KANG • KASTROP • KHASRU • KLINKHAMMER • LANZA CASTELLI
LU MIAO • LÜTKES • MA • MANTHE • MANUEL • MASSA • NARMANDAKH
NOFAL • OLIVER • PINIERO • PURBASARI • QIBTHIYYAH RAHA • RIEFKY
RODRIGUEZ • SAEZ REALE • SATRIAWAN • SCHAAL • SCHULZE
SINGH SITORUS • SNOWER • SONGWE • TIAN • VILLAGRA-DELGADO
WALTENBERG • WANG • WILDNER • YAO • YOON • ZEN • ZHANG • ZHOU

Inequitable Access and Cyber Threats

Policy Brief

Authors:

Prof. Syed Munir Khasru
Chairman, The Institute for Policy, Advocacy, and Governance (IPAG)

Damien Manuel
Chairperson, Australian Information Security Association (AISA)

Ashutosh Chadha
Director and Country Head India – Government Affairs & Public Policy, Microsoft

Abhishek Singh
Director, Digital Transformation, The University of Adelaide

Institutions:

IPAG

The Institute for Policy, Advocacy, and Governance (IPAG) is an independent, international think tank with focus on economic development & trade, technology & innovation, sustainable development and climate change, energy & environment, international relations & strategic affairs, migration & settlement.

AISA Australian Information Security Association

As a nationally recognized not-for-profit organization, the Australian Information Security Association (AISA) champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia.

Social media:
LinkedIn:
www.linkedin.com/in/syed-munir-khasru/

Keywords:
digital divide, internet access, cyber threat

Microsoft

Microsoft's mission is to enable people and businesses throughout the world to realize their full potential by creating technology that transforms the way people work, play, and communicate. Microsoft develops and markets software, services, and hardware that deliver new opportunities, greater convenience, and enhanced value to people's lives.

THE UNIVERSITY of ADELAIDE

The University of Adelaide is a member of Australia's prestigious Group of Eight research-intensive universities, which stands tall among the world's leading institutions of learning and innovation. The University is organized into three academic faculties and six administrative divisions. The university is consistently high rated by the most respected international assessment bodies that consider them one of the top 1% of universities worldwide.

ABSTRACT

The COVID-19 pandemic accelerated global digital transformation, resulting in the manifold benefits such as increased connectivity, boosted productivity, and innovation impetus. The transformation also highlighted the uneven access to digital products and services. According to the World Bank, approximately 40% of the world population is still unconnected to the internet,[1] with the majority living in developing countries. This lack of internet access is attributable to several factors including the absence of digital infrastructure and technology, high costs, and prevailing distrust in technology.

Uneven access to digital products and services also has major implications for the digital economy and cybersecurity. Digitalization of goods and services has the potential to contribute to developing economies. Conversely, increased digitalization risks a rise in cyber-attacks and data breaches. A report by Cybersecurity Ventures estimates that global cybercrime will cost businesses USD 10.5 trillion in 2025 – growing by 15% a year.[2] This is a major concern for both businesses and individuals. While these attacks can lead to the theft of sensitive information, including financial and personal data, they will also decrease trust in technology with debilitating effects on its adoption.

These challenges must be addressed by policy reforms at both the national and international level; firstly, by recognizing the challenge posed by the digital divide. The digital divide is not yet considered a problem in many countries, causing minimal action from governments. This policy brief (PB) will highlight how the digital divide could prevent countries from achiev-

ing economic prosperity and keeping up with global goals, like the Sustainable Development Goals (SDGs). This PB will emphasize the need for undertaking actions for strengthening technological infrastructure and improving internet affordability. The importance of technological standardization calls for cross-country collaboration and agreed norms to prevent harmful use of technologies, cyber-attacks and malicious software. Equally important is for governments and international platforms like the G20 and G7 to come together in promoting high-tech products, like artificial intelligence, machine learning, and the online economy, to unleash creativity while safeguarding privacy, security, and individual rights.

»The digital divide could prevent countries from achieving economic prosperity and Sustainable Development Goals (SDGs).«

BACKGROUND

The pandemic has catalyzed a transition to digital platforms, proving the importance of access to the internet, a key force for socioeconomic inclusion. Technologies and digital space have led to robust growth in areas like working from home, children's education, social welfare services, telemedicine, and availability of financial products in rural and remote areas. The digital divide affects different populations and groups in varying ways across different socio-economic strata. Advanced economies possess higher levels of digital access than developing economies. Similarly, Sub-Saharan Africa has one of the lowest levels of internet accesses despite having high permeation of mobile money transactions.

A country's inequities, such as income inequity and opportunity inequity, may be further aggravated due to uneven digital access, especially for vulnerable groups. Digital access may be proportionate with productivity, especially in developing countries, as exemplified by businesses with reliable internet access that continued operations during Covid lockdowns.[3] By 2020, 60% of the world population were internet users, according to the World Bank.[4] According to the World Population Review, by 2022, 69% of the world population, or 4.9 billion people, were active internet users.[5] However, this also signifies that the rest do not have internet access, which is often distributed disproportionately both within and across countries.

Lower and middle-income countries experience wider digital disparity, both within their boundaries as well as in comparison to their economically advanced counterparts. Further, lopsided growth results from inequitable attainment of development goals across the globe. Vulnerabilities in cyber space are also a major challenge which may result in cyber threats ranging from phishing attacks to cyber terrorism. Governments, private organizations, other entities, and individuals face significant cyber threats in the digital space.[6]

Lack of digital equity also contributes to lack of digital hygiene practices which can expose citizens and businesses to cyber threats. Cyber breaches have varying degrees of impact ranging from economic, financial, and reputational damage. Theft of corporate or sensitive government information can result in security breaches and put lives, property or even economies at risk. The economic cost of cyber breaches includes theft of government information, theft of financial information and money, trade disruption and decrease in business. Furthermore, individuals, businesses, organizations, or governments may fall victim to loss of privacy, or even experience a downturn in business stability and profits.[7]

CHALLENGES

As economies become more digitally driven, the effects of the digital divide are visible in the socio-economic landscape. As digital skills become an integral part of higher skilled jobs, countries or communities excluded from access to the digital space fall behind in accessing the economic benefits of acquiring digital literacy and capabilities.[8] 2.9 billion people are still offline, 96% of whom live in developing countries.[9] Marginalized groups bear a disproportionate disadvantage as the digital divide amplifies prevalent inequities. The digital divide also affects employment and income generation opportunities.

Education is another area in which the disadvantage of the digital divide is felt. The pandemic demonstrated how economies and businesses, which had better access to digital space and technologies, strengthened learning and improved innovation. The pandemic also exposed the digital divide experienced by low-income urban as well as rural communities due to unreliable or unaffordable access.[10] Similarly, while the pandemic showed the power of digital education platforms during lockdowns, it also showed how students or researchers without digital access trailed behind.

The digital divide is disadvantageous to groups with poor internet access as the internet is a large source of knowledge, and Information and Communication Technology (ICT) tools increase learning and research potential. As the digital space influences social interactions through social media and other digital platforms, people, organizations, or communities with poor digital access are excluded from wider global opportunities for social interactions and networking, including professional and cultural recognition.[11] Similarly, inequitable access/adoption of digital technologies by micro, small and medium enterprises (MSMEs) restrict market access and supply chains, which has a detrimental impact on business.

Inequitable digital access hinders SDG achievement. SDG 1, related to eliminating poverty, is impacted as the digital divide aggravates economic inequities by limit-

»Digital inequity contributes to lack of digital hygiene practices, exposing citizens and businesses to cyber threats.«

ing access to economic, educational, and employment opportunities. SDG 3, related to good health and well-being, is affected as access to digital health services has become crucial. While targeted digital health initiatives may benefit some communities, inequitable effects can also result from oversights or the economic disadvantages of nations. For example, an advanced economy may quickly benefit from uses of digital health, as opposed to a lower-income country with limited digital health services. A similar problem exists for SDG 4, which relates to access to education, or SDG 9 which relates to industry and innovation.

»Providing access to digital products, promoting digital literacy, and integrating digital governance is the way forward.«

Inequitable access to technologies and infrastructures translates to inequitable opportunities, especially for lower- and middle-income countries as class, race, and gender gaps are heightened. Internet and mobile banking, microcredits, community online platforms, and market access are examples of meaningful technological solutions to achieve financial inclusion. Problems particular to remote or vulnerable communities can be addressed by targeted investments and efforts to realize access to microcredit or internet banking, and community-centric online platforms such as those for care of the elderly and people with disabilities. For instance, rural agrarian women who require access to financial products or even people caught in humanitarian emergencies can benefit from digital connectivity.[12] However, in the absence of focused a effort, the digital divide continues to widen.

Digital transformation entails adopting new governance, business, and operational models alongside new technologies, requiring investment and organizational efforts. From poor finance availability to inadequately skilled human resources, many challenges persist. There exists a need to foster a shift in mindset, cultivate digital literacy, allot resources, develop infrastructure, and ensure robust feedback mechanisms to create an equitable and secure digital space.[13] The challenges are compounded by cyber threats that present risks to digital capabilities and facilities. Governments and organizations must protect platforms with robust security systems by establishing policy, structures, and monitoring and reporting mechanisms. It is essential to have multiple authentication solutions and other technological remedies.[14] The storage must be based on a "needs basis" and access to sensitive data must be directed by regulatory controls and guidelines.

RECOMMENDATIONS

The reasons for the digital divide can be classified into three main issues: an access divide, an availability divide, and an applicability divide. The access divide, including affordability concerns, which arises from socio-economic differences, requires investments and infrastructure facilitation. The availability divide, which arises from language or other such barriers, limits usage of digital technologies and services, even when they are accessible. Progress made in closing gaps in areas such as gender and disability will be key in reducing the availability divide. Conversely, such a usage divide also arises from a lack of digital skills for which skill development is essential. Applicability, which refers to the aptness of the available technologies, determines the quality of digital usage. Such a gap also stems from poor digital literacy or lack of knowledge.[15]

Policies to promote affordability in accessing the internet and technologies are central. Governments must facilitate the establishment of infrastructure in relevant locations. While advanced economies must ensure that telecommunications infrastructure is set up with minimal urban-rural gaps, emerging economies need to promote infrastructure facilitation overall without neglecting socio-economically challenged communities.

Governments must encourage private organizations, entities, and citizens to avail infrastructure facilities at incentivized rates. Further, government policy must redirect investment into telecommunication infrastructure and developments, with specific provisions to promote private investments. Promoting internet availability to businesses by increasing access to financial products is an example.[16] The use of technology and cyberspace must conjoin trust and good cyber hygiene practices.

An apt regulatory mechanism must guide businesses and education toward bridging the digital gap. Targeted investments in skills development, including integrating digital literacy in primary, secondary, and tertiary education can be promoted to bridge the gap in digital literacy, enhance digital skill competencies, and inculcate the capacity to discern the right knowledge. Governments can also offer job upskilling as well as monetary and other incentives.

»G20 and G7 cooperation on digital development is crucial, now and for the future.«

Since the digital space is an economic platform unbound by geographical territories, it is in the interests of all governments to encourage growth cooperation in bridging the digital divide. The cooperation of trade blocs and economic forums such as the G20 and G7 on digital development is crucial, now and for the future. Knowledge and technology exchange agendas must be broadened across blocs and transnational development agencies. Access to digital products and hardware, promoting digital literacy, and policy to promote and integrate digital governance is the way forward.

Opportunities for cross-border cooperation and growth, and public-private partnerships must be created for addressing cyber threats. Apart from enabling robust cybersecurity practices, cross-border col-

laboration among countries and across government and private sectors must ensure the sharing of threat intelligence, leveraging data sharing and AI to track cyber criminals and disrupt cybercrime activity. Building the requisite framework, including development of cybersecurity professionals, is also significant. At a national level, robust software solutions and optimum infrastructure, along with a regulatory governance structure, are needed to ensure minimal vulnerabilities in the cybersecurity realm.

Encouraging public-private partnerships allows flexibility in building resilient software and hardware solutions. A standardized security code must be developed and implemented for ensuring maximum security in the global network – from the level of private individuals to across governments. Careful consideration must be ensured in the standardization process, concerning the requirements of all stakeholders including developing economies and marginalized communities. Further, a monitoring system along with provisions for receiving feedback and simultaneously fine-tuning systems are prerequisites.

Strong systems will limit criminal activities regarding sensitive government data, which even has the potential to topple economies. However, risks affecting the larger population such as identity theft, data theft, financial theft, impersonation, operational disruptions, and systems compromise must be dealt with in the three-fold manner of implementing protocols for prevention, monitoring, and penalizing offenders. It is essential that national and international policies are congruent, as the goal of ensuring cybersecurity is global.

CONCLUSION

In a world that is progressively becoming digitalized, economic and personal transactions require deliberate action to ensure that cyberspace is equitable and safe. To utilize the great tools that humanity has at its disposal, the digitally equipped world must strategize to minimize the risks while maximizing their adoption. Though the learning process may occur in tandem with the progress of digital transformation, using technology in the most constructive way is of paramount importance. The risks of uneven access and cybersecurity threats are the other side of the coin which may dampen the adoption of digital transformation products and services. The challenge for policymakers is to provide safe and secure digital access to those who are left behind, while ensuring that their legitimate socio-economic aspirations are not jeopardized by the risks and threats that lurk in the cyber world.

1 https://data.worldbank.org/indicator/IT.NET.USER.ZS

2 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

3 https://www.imf.org/en/Blogs/Articles/2020/06/29/low-internet-access-driving-inequality#:~:text=The%20lack%20of%20universal%20and,have%20more%20limited%20Internet%20access.

4 https://data.worldbank.org/indicator/IT.NET.USER.ZS

5 https://worldpopulationreview.com/country-rankings/internet-users-by-country

6 https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity

7 https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

8 https://ctu.ieee.org/economic-effects-of-the-digital-divide-unlocking-growth-with-equitable-access/

9 https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/

10 https://www.weforum.org/agenda/2021/01/covid-digital-divide-learning-education/

11 http://www.digitaldividecouncil.com/the-impacts-of-digital-divide/

12 https://www.nature.com/articles/s41467-021-26217-8

13 https://pecb.com/article/digital-transformation-challenges-and-how-to-overcome-them

14 https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity

15 https://www.iberdrola.com/social-commitment/what-is-digital-divide

16 https://www.imf.org/en/Blogs/Articles/2020/06/29/low-internet-access-driving-inequality#:~:text=The%20lack%20of%20universal%20and,have%20more%20limited%20Internet%20access.

THE WORLD POLICY FORUM

ISSUE 9 • MAY 2023

For full journal, please click on:

https://www.global-solutions-initiative.org/wp-content/uploads/2023/05/Global-Solutions-Journal-9-Summit-2023-Edition.pdf