Technology, Security, and Transparency

This policy brief proposes strategic solutions to some of the most pressing digital technology challenges faced at a global level. Two cross-cutting recommendations will strengthen all policies and programmes designed to regulate technology. Education of emerging technologies for beneficial use and mitigation of potential harm and collaboration between stakeholders and countries to deal with the ever-evolving digital environment and promote a secure and inclusive digital world.

Our thematic recommendations include:

- **Technology for Empowerment** We advocate for enhancing accessibility and inclusivity by setting up infrastructure bridging the digital divide, promoting user-centric design in technology, establishing open-data policies, democratising e-commerce platforms, and investing in robust technological solutions to achieve the SDGs and creating an inclusive and fair digital society.

- **Security, Safety, and Resilience** This theme underscores the importance of international cooperation and collaboration in cybersecurity, protection against cyber attacks on critical infrastructure, establishing legal frameworks to counter online violence, especially toward vulnerable populations, and developing norms to prevent misuse of AI systems and regulating technologies that innately induce addictive tendencies and negatively affect user's health and well-being.

- **AI and Data for Society** We emphasise that ethical, fair, and safe deployment of technology must be ensured, the generation of high-quality datasets for marginalised communities is incentivised, and international regulations assigning liability for harms arising from technology are created.

- **Transparency, Trust, and Disinformation** We propose measures to combat disinformation, including developing a shared terminology and a comprehensive strategy, establishing national information networks, establishing an effective legal infrastructure, and enhancing transparency and trust within the technology supply chain.

The recommendations provided in this policy brief aim to create a digital future that is more accessible, secure, transparent, and inclusive. A future that leverages technology to create safer, more equitable societies globally.

Introduction

Technology has transformed how we interact with our surroundings and with each other. Automation, digitisation, and computerisation have increased productivity and convenience in our daily lives. The internet and digital technologies have revolutionised how nations approach challenges and transformed the global economy. Digital literacy has become a prerequisite for most workforce sectors, allowing people to transition from low-skill to middle-skill jobs. However, technology can exacerbate inequalities. Despite the benefits, the availability and accessibility of technology are not evenly distributed, with underdeveloped countries and less developed regions within developed countries being left behind. Although the digital economy is challenging to measure, it has become a significant propellant for commerce. There is now unprecedented dependence on the access, quality, and integrity of digitised information.

1. The digital economy is the primary catalyst for economic progress in developed and underdeveloped countries; hence, these issues must be addressed.

2. Ensuring accessibility and availability of technology is essential, but it is equally important to address significant security issues collectively. Technology has been weaponised in various ways, including spam mail with viruses and spear-phishing campaigns. Deep learning techniques can be misused to develop tools for harm, such as: propaganda, manipulation, and economic warfare. Cyber attacks are increasingly prevalent, with an expected annual cost of 10.5 trillion USD by 2025.

3. Moreover, inadequate security and privacy is a growing concern, and the dissemination of disinformation has aggravated societal divisions and polarised the world. It is causing severe harm to individuals and socio-political stability. Youth, in particular, are facing unforeseen effects living in a digital

world, including online harassment, cyberbullying, and internet overuse, affecting both their mental health and physical well-being. In addition to these challenges, Artificial Intelligence (AI) has brought new ethical concerns, bias, lack of transparency, and potential job displacement. These issues are classified as global risks by the World Economic Forum.

4. The fast pace of new technology development and consequent releases have outpaced the ability of policymakers to adapt and regulate them effectively. Civilians are the most impacted by emerging paradigms in technology development and use. There is a pressing need for online spaces to remain secure, safe, and lawful and ensure transparency in the policies that govern digital technologies. The C20 Technology, Security, and Transparency (TST) Working Group addresses these various technology-related risks, opportunities, and challenges society faces through the following policy recommendations.

Cross-Cutting Recommendations

1. Education of emerging technologies for beneficial use and mitigation of potential harm is key to success. G20 countries should prioritise financial and human resources to design and implement comprehensive awareness and educational training programs. This education must cater to different age groups for digital up-skilling and reskilling on emerging technologies and provide an understanding of their impacts. This requires collaboration between the public, private and civil society sectors, with input from experts to develop tailored curricula and training activities to exercise critical thinking and increase competency. Those with limited financial capacity, low-income occupations, and those living in low or no-access rural areas should be prioritised. These training programs should integrate ethics and ensure that citizens of all ages can understand, safely use, and adopt new and upcoming technologies. Monitoring, evaluation, and national reporting of these programs should be integrated into programme design to measure their effectiveness and ensure they remain relevant and up-to-date with the rapidly evolving digital landscape.

2. Collaboration between stakeholders and countries is required to deal with the ever-evolving digital environment and promote a secure and inclusive digital world. We call on political will, leadership and action to encourage cross-border cooperation among governments, international organisations, private industries, academia, and civil society towards:
a). The creation and implementation of multi-stakeholder frameworks, protocols, and standards that ensure policy coherence, consistency and facilitate information sharing, capacity building, and collective action and
b). Support the exchange of best practices, expertise, and technologies, establish trust, promote responsible behaviour, and uphold digital rights, inclusivity, and security through these frameworks. Moreover, it is essential to actively involve all stakeholder groups, including those from marginalised groups, in shaping policies and programs.

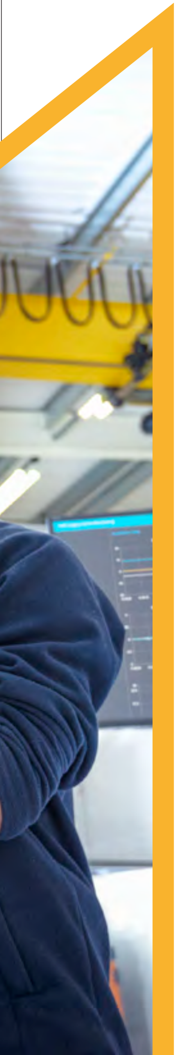
I. Technology for Empowerment

Technology is now a fundamental pillar of our society. The economies of all countries are reliant on technology; hence empowering people with technology increases possibilities for the future. Three primary challenges have been identified concerning the digital economy.

1. Lack of accessibility, availability, and affordability inhibits sustainable development and the betterment of society. Physical infrastructure development is a barrier in rural areas where internet use is only 46% compared to 82% in urban areas.

2. For persons with disabilities, it is essential to have accessible technologies to participate in the digital ecosystem and achieve financial independence and resiliency.

3. Approximately 61% of all online content is in English. Parity in access to the digital world in low-English proficiency countries can only be achieved through the enablement of multilingual internet. For this, content in local languages and Universal Acceptance (UA), internationalised domain names (IDNs) and Unicode are necessary.



Technological solutions can help reduce global imbalances; for example, digital payment systems can increase financial inclusion. Another example is open-source initiatives allowing access to Information and Communication Technologies (ICT) by providing free, flexible, and customisable technology for developing countries and marginalised communities. Improved access to research publications is also important for society’s prosperity.

However, access is frequently limited due to paywalls or fees for access. In some cases, access to necessary technology can be impeded by patent regulations and the reluctance of some organisations to share information, citing proprietary or competitive interests, hindering essential information sharing necessary for the common good and preservation of humankind, best exemplified by the COVID-19 vaccine.

Policy Recommendations

- Align with the UN's universal connectivity goals by promoting policies that expand broadband connectivity and access to digital devices, especially to remote, underserved, and vulnerable communities by 2030. Support multilingual internet by adopting UA, IDN and Unicode.

- Ensure that critical digital technologies such as financial, governmental, and healthcare services are inclusive and accessible for persons with disabilities by promoting user-centric design and establishing audit mechanisms to enforce accessibility guidelines. Mandate subsidising import duties and taxes to make assistive technologies affordable by 2027.

- Integrate digital unified payment interfaces to significantly accelerate the growth and adoption of the digital economy while enhancing financial inclusion and economic empowerment.

- G20 countries must incentivise, promote, and develop open-source software that enables long-term, customisable technology solutions at minimal cost for public procurement. At least 40% of new software contracts in government should be open-source software by the year 2025.

- Mandate publicly funded non-classified research to be available as part of the digital commons to benefit the public, industries and academia.

- Digital platforms for e-commerce should be democratised and regulated by a public authority to ensure open and fair digital commerce practices that benefit Micro, Small and Medium enterprises (MSMEs).

- G20 countries should incentivise investments in vital technological innovations that preserve life and ecosystems. Speeding up the distribution and sharing of these technologies is crucial to achieving the Sustainable Development Goals (SDGs) by 2030. Furthermore, we recommend that governments subsidise these technologies to facilitate their accessibility for the least-developed countries.

II. Security, Safety and Resilience

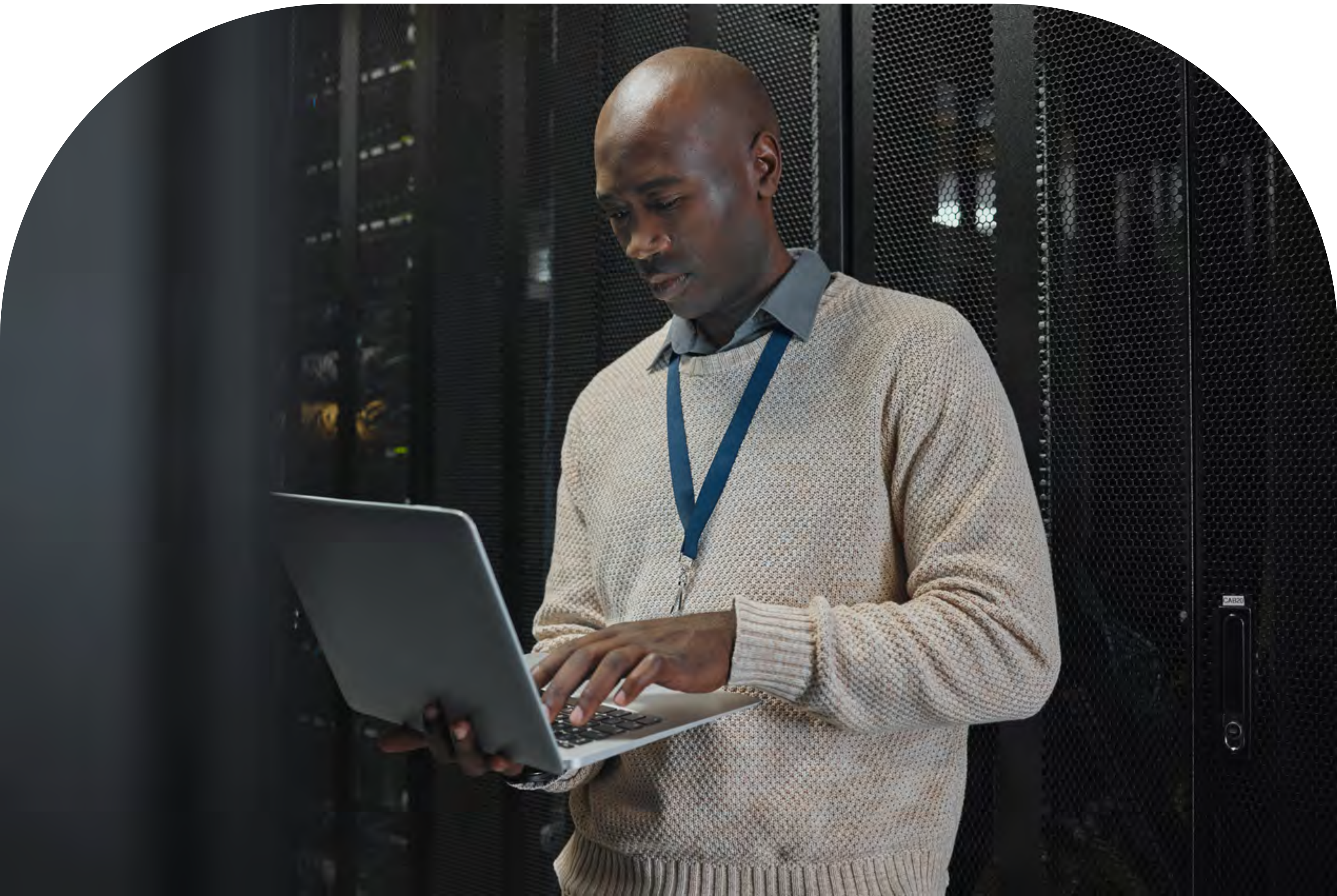
Widespread cybercrime and cyber insecurity are among the top 10 global risks. Governments, businesses, regulators and consumers are placing strategic priority on safeguarding technology ecosystems against cyber threats. While designated organisations must collect and use data to combat cybercrime and terrorism, balancing cybersecurity policies with individual rights is crucial. With the Second Additional Protocol to the Convention on Cybercrime, CSOs have expressed concern about the privacy risks posed by data sharing.

Addressing cybercrime can pose significant challenges due to the anonymous nature of virtual attackers. Targeting critical infrastructure and causing disruption of essential services such as power grids, water systems, health facilities, financial systems, and all vital services through cyber attacks can cause a colossal impact with significant ramifications to society.16 The increasing complexity of cross-border cybercrime makes coordinating a response challenging, necessitating stronger international cooperation and information sharing between multiple stakeholders.

The majority of the general public often have limited awareness or understanding of the ever-changing landscape of cyber threats. Vulnerable populations, including the elderly, persons with disabilities, and children, are more susceptible to online threats, such as cyberbullying, asset and identity theft. Due to scarce resources, there is also a lack of cybersecurity resilience among CSOs and businesses, especially in MSMEs. The average cost of data breaches varies between 38,000 USD and 4.35 million USD, depending on the organisation's size.

Cybersecurity risks threaten AI systems making them prone to error or theft and potentially destructive. Moreover, AI systems make decisions using complex functions, making it difficult to ensure transparency and explainability. These challenges are not limited to specific industries or applications but pervasive across all AI implementations and products.

As we rapidly iterate and build new technologies, we must also consider the potential negative side effects of technology that can induce overuse and potentially negatively affect users' mental and physical health.



Policy Recommendations

- Increase international cooperation in cybersecurity as provided in the Budapest Convention.

- Fund and develop designated nodal agencies to enhance collective defence towards cyber threats and implement preventative measures. Facilitating collaboration between governments, the private sector, and other stakeholders is crucial to increase cybersecurity incident reporting.

- Enhance national cybersecurity policies and define mechanisms to enforce international standards and measures to safeguard cyberspace while respecting and protecting human rights.

- G20 countries should collectively recommend an additional protocol to the Geneva Convention specifically prohibiting any state from engaging in cyber attacks on critical infrastructure systems affecting civilian safety during conflict.

- Enhance cooperation between government, the judiciary, law enforcement and technology companies to mitigate online exploitation, violence or cyberbullying, especially towards children, women and persons with disabilities. Strengthen institutional mechanisms, enact comprehensive legislation, allocate resources for specialised units towards prompt investigation, impose stringent penalties, and enforce strict content moderation by 2028.

- Establish regulatory guidelines that ensure new technology releases safeguard users' physical and psychological well-being by conducting comprehensive analyses of potential negative side effects before their releases. This is especially relevant to the gaming and social media industries, whose user base is more susceptible to technology overuse.

- Develop a broad-ranging set of cybersecurity norms for AI systems, adaptable to the safety-critical nature of AI products, to prevent misuse of AI by malicious entities.

III. AI and Data for Society

2023 is likely to be remembered as the year ChatGPT, an AI language model, became a household name. The potential applications of AI are numerous, including healthcare, accessibility, research, business, and overall economic growth. It is predicted that by 2030, 70% of organisations will be using at least one type of AI technology. AI is expected to contribute 15.7 trillion USD to the global GDP by 2030. While AI technologies have been under development for many years, little regulation has been developed to address the considerations required for a safe and harmonious society. Efforts such as UNESCO's recommendations on integrating ethics in AI are broad, far-reaching, and exhaustive. However, they have not been translated into concrete legislation.

One of the most significant issues in AI is the proliferation of bias and discrimination, reflected in AI algorithms and systems due to human biases and systemic inequalities collected into the datasets used to power AI. These biases lead to unfair or inaccurate decision-making, disproportionately affecting marginalised groups. While datasets are not the sole cause of bias, they are a dominant factor. Another possible risk is sensitive data leakage. Using external third-party systems may lead to mishandling personally identifiable information (PII) and similar information.

Policy Recommendations

- Develop policy mechanisms and regulatory measures to ensure that data collection and technology development are deployed and used ethically, fairly, and safely in accordance with the OECD value-based AI principles.

- Incentivize and mandate the generation of high-quality datasets for and from marginalised and underrepresented communities to correct biases in medical, financial, economic, and all generative AI applications. Foundational and current datasets should be collected, debiased, and verified by established teams of experts and stakeholders to ensure inclusivity and impartiality by 2028.

- Establish international regulations that explicitly assign liability for harms arising from technology to ensure accountability and protect users' rights and interests. It is crucial to foster collaboration between international legislative and judicial systems, technology corporations, civil society, and independent regulatory bodies; to prescribe policies for non-compliance and dispute resolution mechanisms that are fair and impartial.

IV. Transparency, Trust and Disinformation

Disinformation has become a significant threat to today's society. While costing the world a staggering 78 billion USD annually, its impact has grown significantly with the advent of social media. With 4.8 billion users, social media platforms have become primary vehicles for spreading disinformation and polarising content. False information spreads faster on these platforms than accurate information, leading to the division of populations and increasing tensions among citizens.

Economists have recognised the correlation between trust and increased GDP. The potential risks of disinformation jeopardise the political stability and trust in established systems. Disinformation sows confusion and a lack of trust in established systems such as healthcare and scientific communities, as seen in the recent COVID-19 pandemic. It is crucial to develop approaches to address both dissemination of and response to disinformation without compromising human rights.

Moreover, the global technology supply chain, encompassing hardware and software presents a range of challenges. Recent supply chain incidents such as the WannaCry and SolarWinds attacks impacted organisations in over 150 countries, causing over 94 billion USD in losses. Adulteration, counterfeiting and sub-standard products are other manifestations of deficient supply chain processes that could be mitigated using technology. Addressing these concerns is vital to maintaining our global marketplace’s safety, security, and reliability.

Policy Recommendations

- Facilitate global cooperation towards ending the spread of disinformation. Create a shared terminology and produce a comprehensive strategy against the spread of disinformation in congruence with UN General Assembly resolution 76/227.

- Establish national information networks that include professionals, news, and social media teams to track and respond to misinformation and disinformation.

- Develop an effective legal infrastructure to transfer the financial burden of the fight against disinformation to the individuals or entities responsible for its creation and propagation as set in national laws and regulations.

- Design and implement a trusted network for technology procurement, specifically focusing on G20 nations’ supply chain.

Udaaharans

GLIDES

The Global Internet Governance, Digital Empowerment and Security Alliance (GLIDES), is an alliance of Civil Society Organizations (CSOs) and the first of its kind. It is an alliance and a launchpad for multi-stakeholder policy-making processes toward security and internet governance. This alliance focuses on digital access, internet governance, inclusivity, online safety, net neutrality, data privacy, data governance, fake news, multilingual internet, and digital rights.

Team4tech

Team4Tech is a nonprofit impact accelerator, bridging the digital equity gap in education to foster inclusion and create opportunities for under-resourced learners worldwide. Team4Tech partners with companies on social impact projects that provide technology grants and training to build nonprofit capacity and provide opportunities for learners around the world.

Shakticon

ShaktiCon is an initiative for women by women that has successfully served as a platform to inspire, train, and upskill women in cybersecurity by providing an inclusive environment that showcases female talent and promotes diversity. ShaktiCon has mentored over 5,000 beneficiaries from over 70 countries worldwide in the past five years, contributing to developing a more diverse and skilled workforce.

References

1. https://unctad.org/system/files/official-document/ier2017_en.pdf

2. https://www.frontiersin.org/articles/10.3389/fpubh.2022.856142/full

3. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

4. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

5. https://www.itu.int/hub/publication/d-ind-ict_mdd-2022/

6. https://www.orfonline.org/expert-speak/when-a-bridge-becomes-a-wall/

7. https://www.un.org/esa/ffd/wp-content/uploads/2016/01/Digital-Financial-Inclusion_ITU_IATF-Issue-Brief.pdf

8. https://www.itu.int/hub/2022/04/new-un-targets-chart-path-to-universal-meaningful-connectivity/

9. https://www.w3.org/WAI/standards-guidelines/wcag/

10. https://c20.amma.org/tst-wg/global-internet-governance-digital-empowerment-and-security-alliance-glides/11 https://team4tech.org/

11. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

12. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224

13. https://edri.org/wp-content/uploads/2023/04/Civil-society-Open-letter-to-protect-encryption.pdf

14. https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human

15. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

16. https://press.un.org/en/2022/gashc4344.doc.html

17. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

18. https://www.ibm.com/downloads/cas/3R8N1DZJ

19. https://learn.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning

20. https://rm.coe.int/1680081561

21. https://www.shakticon.com/

22. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI-frontier-modeling-the-impact-of-ai-on-the-world-economy

23. https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

24. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

25. https://oecd.ai/en/ai-principles

26. https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

27. https://www.statista.com/statistics/617136/digital-population-worldwide/

28. https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308

29. https://www.oecd-ilibrary.org/sites/9789264307278-12-en/index.html?itemId=/content/component/9789264307278-12-en 31 https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry

30. https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided