A Blueprint for Inclusive Digital Co-ordination

Policy brief

Author:

Catherine Mulligan
Co-Founder, Emerging Technologies Sustainability Taskforce and Visiting Lecturer, Imperial College London

Institution:

ETST

A team of experts spanning Accounting, Technology, and Sustainability, with a keen focus on promoting the sustainable utilization of technology, ETST was created to fill the recognised the need for a transdisciplinary approach to the world of standardisation. ETST has a strong focus on the real-world usability of the standards created and exists to transform how digital technologies are used to create sustainability outcomes.

Keywords:
standardization, inclusive growth, digital technologies, digital coordination

Globalization and rapid technological change have reshaped the global landscape, ushering in opportunities and challenges. The resurgence of protectionist sentiments and apprehensions surrounding future technologies underscore the complexities of navigating this new era. Most of the global focus recently has been on AI. However, this misses many other technologies that should be addressed with AI as a suite of technologies rather than separately. Amidst this complex backdrop, digital technologies are often seen as pivotal in achieving the Sustainable Development Goals (SDGs). While digital technologies hold immense promise in addressing the SDGs, the proliferation of such initiatives introduces uncertainties in an evolving multipolar world order, which the G20 must appropriately consider.

Many global initiatives have been launched that aim to facilitate the equitable distribution of digital technologies and emphasize digital technologies' role in alleviating poverty and fostering inclusive innovation. Not least among these initiatives is the Digital Public Infrastructure (DPI) work supported by the G20. The G20 is, therefore, trying to assume a pivotal role in fostering constructive relationships and forging models of global cooperation concerning digital technologies. This policy brief delineates three main recommendations for the G20 to navigate the complexities of global technology governance, ensuring it facilitates inclusive pathways to prosperity while safeguarding security and privacy. Rather than focus on one initiative specifically, it focuses on digital technologies applied at the government (nation-state) level as part of Critical National Infrastructure (CNI), with a specific focus on creating inclusive growth and co-creation of solutions.

»Due to the increasingly complex nature of digital technologies and increasing geopolitical instability, a more structured approach to co-creating digital solutions is necessary.«

Firstly, it addresses the G20's role in formulating effective strategies to combat disinformation and bolster digital intelligence alliances. Secondly, it outlines engagement strategies that ensure middle powers (aka the Global South) are included as equals in these processes. Strengthening these alliances by including middle powers is imperative to safeguarding global peace. Finally, it proposes a blueprint of global cooperation for technology, which builds upon past successes while managing the inherent challenges associated with digital technologies. The G20's proactive engagement in shaping global technology governance is imperative for navigating the complexities of the digital age, particularly when digital technologies are used as critical infrastructure. Through strategic collaboration and inclusive poli-

cymaking, the G20 can pave the way for a future where digital technologies catalyze sustainable development and shared prosperity. As many other multilateral systems, such as the UN, struggle to deliver on their mandates, the G20 can play a strong coordinating role in the emerging world order.

I. INCLUSIVE DIGITAL INNOVATION

Over the last decade, several waves of technological innovation – IoT, Blockchain, Metaverse, and AI, have all been proposed as solutions to the world's problems. The latest focus has been on AI, while a few years ago, the regulatory focus was on Blockchain. With each new technology, governments and regulators struggle to respond. This is because each new technology is treated separately as its own General-Purpose Technology (GPT). Viewing the technologies as an infostructure instead of as individual technologies enables a more robust discussion and allows high-order regulation and global coordination. Moreover, many of the newer technology solutions proposed to solve the SDGs are not just government systems or corporate systems, but they are systems that include citizen IDs, payments, and biometrics. As such, these systems are not traditional IT systems and, as such, should be treated as Critical National Infrastructure (CNI); i.e. infrastructure considered essential by governments for the functioning of a society and economy and, therefore, deserving of special protection for national security.

A comparison could be drawn to the regulatory environment for Pharmaceuticals – which focuses on ensuring the "safety, efficacy, and quality of the drugs available to consumers" (Olson, 2014). It does this by focusing on the overall impact of entire drugs, rather than focusing on one chemical compound within it. Rather than creating separate regulations for AI, Cryptocurrency, or Social Media platforms, which is the equivalent of focusing on only one chemical compound in a drug, technology regulation should instead be looking at the overall impact of the technologies within the infostructure. Taking an infostructure approach to regulation would allow easier alignment between regions and nations and create similar regulatory goals. Following Pharmaceuticals' example, regulation of the infostructure could include guiding principles such as "secure, democracy-preserving, high-quality", which would be set by the G20.

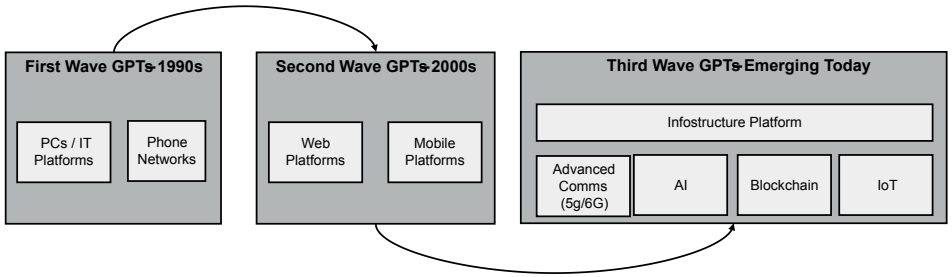

Figure 1: Several Waves of General Purpose Technologies

Underlying the infostructure is data; IoT solutions are only usable with data analysis and, increasingly, AI. Blockchain solutions, meanwhile, are not useful without storing transaction data. Data has become a new factor of production – it is now a critical input to many goods and services of the 21st century. Most companies working with the large-scale collection, storage, and processing of this new factor of production for the global marketplace are headquartered in one nation – the USA. The companies associated with the data as a factor of production economy are commonly referred to as MAGMA – Meta, Amazon, Google, Microsoft, and Apple. Amazon has a market cap or net worth of $1.79 trillion as of March 12, 2024, Microsoft a little more than $3 trillion, and Apple's market cap is just under $3 trillion. Alphabet (Google) has a market cap or net worth of $1.69 trillion as of March 12, 2024 (Data source: Statista, 2024). As illustrated in Table 1, this is significantly higher than the market caps of many nations; only seven countries have higher market caps.

»These solutions should be treated as Critical National Infrastructure (CNI) - infrastructure considered essential by governments for the functioning of a society and economy.«

Therefore, another critical issue for the G20 is enabling an even distribution of the benefits and revenues of such technologies.

CONCRETE RECOMMENDATIONS:

- G20 should approach digital technologies from a holistic perspective, rather than regulate technologies individually.

Rank	Country	GDP (Trillion USD)	Market Cap (Trillion USD)	GDP per capita	Share of GDP
1	USA	25.463	50.8	75,269	25.32
2	China	17.963	12.2	12,598	17.86
3	Japan	4.231	6.36	34,135	4.21
4	Germany	4.072	4.07	48,845	4.05
5	India	3.385	4.5	2,389	3.37
6	UK	3.070	2.4	45,485	3.05
7	France	2.783	3.9	43,061	2.77

Table 1: Market Cap and GDP of Nations (Data source: World Bank, 2023)

- G20 should set globally recognized guidelines for the application of digital technologies that have an impact on the nation-state.
- G20 should foster globally interoperable regulatory regimes by approaching regulation from the lens of an infostructure.
- New methods of global collaboration should be sought that enable a globally inclusive approach to revenue generation from data.

II. BUILDING DIGITAL COOPERATION FOR THE 21ST CENTURY

In today's multi-polar world, there is a need to enable regions, countries, and companies to have equal opportunity to input to the development of technologies and equal opportunity for domestic companies to earn money from the data collected from their citizens. Due to the increasingly complex nature of digital technologies and increasing geopolitical instability, a more structured approach to co-creating digital solutions is necessary which:

1) Enables innovation and market creation globally.
2) Equally distributes economic opportunities across all world regions.
3) Ensures the security of the citizens using them.
4) Ensures the agency of each nation to deliver its national security.

Several successful global coordination mechanisms exist within the technology sphere, for example, the standardization processes used for telecommunications, which have successfully enabled global market creation and co-development of solutions for multiple generations of technology. Telecommunications – as a critical national infrastructure itself – can inspire global coordination mechanisms when combined with the benefits of a more IT-driven approach. These processes should be adapted to ensure participation from all regions. A rough blueprint follows. This brief focuses on CNI, however, this process can also be adapted for other multilateral and multipolar governance issues; in short, it can act as a blueprint to enable multilateral cooperation around technology more broadly.

STAKEHOLDERS

In a multipolar world, the technology development process must balance several highly complex stakeholder relationships. These include primary and secondary stakeholders, as illustrated in Table 2 below.

Primary stakeholders include active participants in developing standards, while secondary stakeholders are active in ensuring the standards developed are usable for their needs. Secondary stakeholders traditionally do not actively contribute to the standards but are consulted by relevant primary stakeholders, most often around the requirements. In our scenario, however, civil society organizations and end-user community groups can apply to participate. Due to space limitations, this document focuses on the primary stakeholders and how these can be successfully developed for multipolar technical cooperation, rather than the secondary stakeholders. In contrast to today's standards bodies, operational partners should be drawn from all regions of the globe, enabling a more inclusive approach.

Grouping	Stakeholders	Description
Primary Stakeholders	Corporations	Companies/organizations working on relevant technologies and solutions
	Regional Partner Organizations	Established standards organizations in regions (e.g. ETSI)
	Operational Partners	Should represent each major region— e.g., Europe, Asia, India, the Americas, Africa, and ME. Responsible for ensuring solutions are implemented and tested correctly
Secondary Stakeholders	End-User Communities	Groups with domain knowledge
	Government Departments	Departments with direct interest
	Civil Society Organizations	Groups with domain knowledge
Approval Body	G20 Established Group or one established at the ITU by the G20	This group acts as a final approval for the standards to ensure that there are stable releases

Table 2: Stakeholders for developing inclusive digital cooperation.

The standardization work should be contribution-driven; anyone who participates can contribute documents for review and inclusion. Stakeholders should apply to participate through membership in an Organizational Partner, e.g., the Regional Standards Committees. Specifications would be co-created and co-developed at relevant working groups (WG). WG meetings would be held several times yearly, and contributions would be prepared, debated, and discussed. Those deemed suitable would be included in the final specification.

Specifications would be grouped into "releases", each with an internally consistent set of features and specifications. Operational Partners can then transpose the approved specifications into deliverables.

»Taking an infostructure approach to regulation would allow easier alignment between regions and nations and create similar regulatory goals.«

»The G20's proactive engagement in shaping global technology governance is imperative for navigating the complexities of the digital age.«

Notably, this innovation framework means any company can develop and implement solutions based on these specifications, even those who did not attend the meetings. This enables a stable set of digital critical infrastructure services to be developed and tested for application in national contexts and a secure, stable market for the companies producing them. This process enables a market-creation process between companies, users, and regulators/governments in a multi-sided market.

Due to the requirements for a structured, secure, and stable approach to the delivery of CNI products and services, it would be helpful to adopt a four-stage methodology, adapted from the three-stage methods of the ITU-T (ITU,1998) covering:

- *Stage 1 specifications* define the service requirements from the user's point of view.
- *Stage 2 specifications* define an architecture to support the service requirements.
- *Stage 3 specifications* define an implementation of the architecture by specifying protocols in detail.
- *Stage 4 specifications define test specifications to ensure the system, product, or service works as described.*

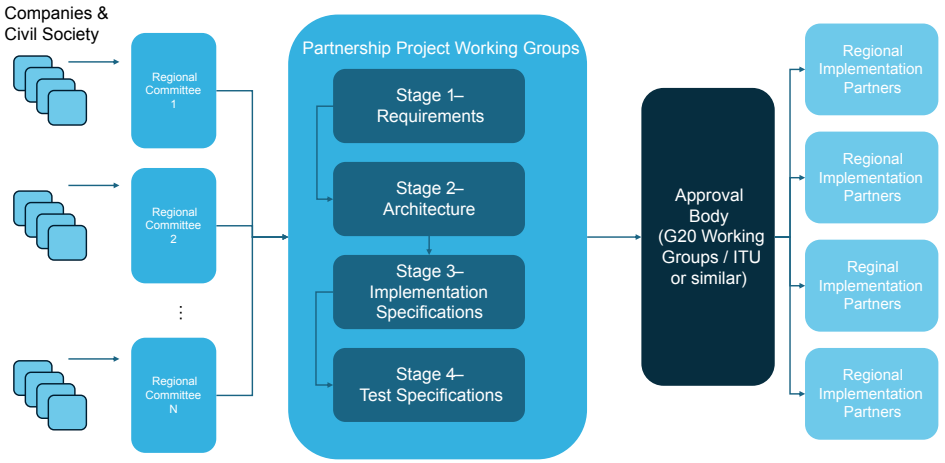

Figure 2: Example Structure for Standardisation of Digital Technologies for CNI

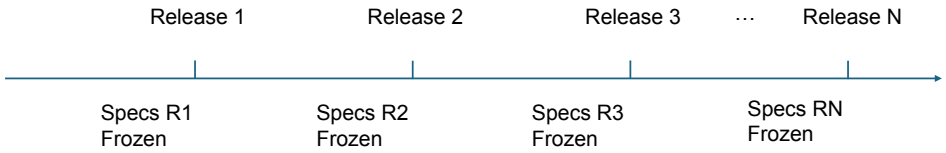

Figure 3: Example Release Freezes over time.

CONCRETE RECOMMENDATIONS:

- G20 should establish a body that runs the standardization process globally for digital cooperation that can ensure the correct parties are involved in the process. This could be done in conjunction with the ITU.
- Capacity building for standards globally should be prioritized so all regions can participate effectively.

III. ALLIANCES FOR CYBER RESILIENCE

One of the most critical areas of cooperation that the G20 should establish as digital technologies are rolled out as CNI is alliances for cyber resilience and national security. Undoubtedly, information wars – specifically those aspects that manipulate information to influence public opinion - are already challenging governmental institutions and growing in number and sophistication (Prier, 2017, Aïmeur et al, 2023). There are also increasing attacks on open-source repositories, which could affect the CNI solutions built using this model (Nelson, 2024).

In previous eras, where national cyber security has been at risk, new forms of international cooperation have been established – two well-known examples are Five Eyes (Australia, Canada, USA, UK, New Zealand) and Fourteen Eyes (Australia, Canada, New Zealand, UK, USA, Denmark, Netherlands, France, Norway, Germany, Belgium, Spain, Sweden, Italy). For those third-party countries that wish to gain access to the intelligence from these alliances, there is an option to pay to receive information. Smaller coalitions today are already working together – e.g. AUKUS works on AI (Luckenbaugh, 2023). However, the ability to scale these types of organizations will be critical to the longer-term success of the use of digital technologies such as CNI.

Cyber resilience at a national security level requires many highly specialized human resources. This capacity building should occur before any of the systems are installed in nations around the world. A failure to properly develop capacity in this regard will increase the threat landscape for other countries.

In addition, nation-states must be able to retain control and agency over their national security. In some instances, placing their government systems under the control of corporations headquartered in other countries could create critical risks, especially in a world with a shifting geo-political landscape.

CONCRETE RECOMMENDATIONS:

- The G20 should implement flexible coordination mechanisms that can manage many nations suddenly becoming "digitally enabled". Loosely coupled alliances could help to protect the overall global infrastructure alongside the more established treaties.

REFERENCES:

Aïmeur, E., Amri, S. & Brassard, G. Fake news, disinformation, and misinformation in social media: a review. Soc. Netw. Anal. Min. 13, 30 (2023). https://doi.org/10.1007/s13278-023-01028-5

Luckenbaugh, J., 2023, AUKUS Partners Advancing on AI, Autonomy, available online:

https://www.nationaldefensemagazine.org/articles/2023/9/20/aukus-partners-advancing-on-ai-autonomy

Nelson, 2024, Millions of Malicious Repositories Flood GitHub, GitHub, and cyberattackers are waging a quiet, automated war over malicious repos., Dark Reading, available online: https://www.darkreading.com/application-security/millions-of-malicious-repositories-flood-github#.

Olson, M. K. (2014). Regulation of Safety, Efficacy, and Quality. In A. J. Culyer (Ed.), Encyclopedia of Health Economics (pp. 240-248). Elsevier

Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly, 11*(4), 50–85. http://www.jstor.org/stable/26271634 ITU, 1998, https://www.itu.int/rec/T-REC-I.130-198811-I/