JESUS COLLEGE
CAMBRIDGE

Global Issues
Dialogue Centre

Discussion Paper

The Dynamics and Direction of Global Digital Governance

Andrew Cainey
Senior Associate Fellow, Royal United Services Institute

Contents

Executive Summary

1. Global governance in all spheres is evolving with many challenges in terms of achieving a common goal through international institutions. Digital governance is in its infancy and to date has had a technical, US-centric focus. Many, if not most, nations are now actively strengthening governance, with issues of economics, national security and values to the fore, alongside technical considerations. This geopolitical context – rather than the established positions of the post-World War II global settlement – defines the space for global digital governance.
2. The pervasive role of technology in society means that investing time and effort to establish effective global governance is an urgent priority. The rise of China and the current geopolitical environment mean that there are differing perspectives on what this looks like and increased competition to shape governance design.
3. Geopolitics is putting pressure on the common standards, knowledge-sharing and research co-operation, trade, investment and globally distributed value chains that have driven much recent innovation and productivity in digital technologies.
4. These pressures risk jeopardising many of the economic benefits of globalisation and integration so as to address concerns on security, risks and differences in values. It makes sense for all countries to find ways to address these concerns and increase mutual trust and so preserve as many of the economic benefits as possible.
5. Agreement on common standards will become more challenging as countries view standards as source of national advantage. Universal standards will win out most easily where they do not bring decisive implications for industrial competitiveness, national security or societal values.
6. A renewed emphasis on national industrial policy in technology requires concerted action to maintain trade and investment openness and a level playing field wherever possible. Left unchecked, the consequence is continued or closer integration with 'like-minded' countries and greater separation in trade and business relations from others ('decoupling').
7. Regulation of Big Tech corporate behaviour has international as well as domestic implications. The approach to regulation and stability of the major global financial institutions may offer some lessons.
8. New trade and investment agreements are needed that help liberalise digital trade, data flows and cross-border use of algorithms. These will be easier to negotiate in smaller country groups and between societies with similar systems of government than on a global basis.
9. Effective governance mechanisms in the field of defence and security are even more challenging to design and to reach agreement on.
10. Most non-state elements of cyberattacks are akin to criminal and terrorist activity with the same potential for global agreements and selective cooperation.
11. Between states, both the scope and the rules of the game in cyberattacks are ambiguous. The scope can include large-scale information-gathering, disinformation campaigns and potential attacks on infrastructure across the entire economy. AI, quantum computing and other new technologies make this all both more dangerous and more uncertain as well as changing the nature of 'traditional' warfare. Bilateral engagement between adversaries to identify the largest risks, reduce ambiguity and agree some rules of the game would bring benefits, though incentives to engage vary. In some areas, a more broad-based approach may both help the

largest countries reach agreement and also lead to worldwide consensus to ban certain uses of technology.

12. Support to lower-income economies has long been an element of global governance. Multilateral institutions need to do more to address issues of economics, security and values – and supporting individual countries in making their own choices on questions of digital governance.

13. As it takes shape, global digital governance will take the form of a complex patchwork of institutions and agreements between countries with both similar and different approaches. This patchwork reflects technology's pervasive role: societal differences matter more than technical standards. The extent of global commonality will both rest on alignment and trust between countries and itself be a mechanism for increasing stability and trust between countries. Where commonality can be agreed, increased productivity and innovation will generate economic returns.

14. The shape and effectiveness of this governance patchwork depends on individual leadership and the actions taken. This calls for a series of parallel initiatives that work with both existing and new governance structures – and build on national digital governance structures that are themselves a work in progress. Progress on cooperative engagement is most likely between like-minded countries. A striking example is the strengthening of G7 and US-EU discussions on technology and potential expansion to other major democracies. Broader initiatives (often UN-centred) remain important to enable more inclusive considerations of key issues but will struggle to effect action directly. Bilateral or minilateral discussions may be most appropriate for some of the most pressing and contentious security-related issues such as cyberwarfare and the militarisation of new technologies, in particular between the US and Russia and the US and China.

I. Introduction: The growing relevance of digital governance

Digital technology today affects all aspects of society and daily life, yet the governance of this technology remains a work in progress.

The term 'governance' is itself frequently used and less frequently defined. One almost-tautologous definition is 'the act of governing something'.[1] UNESCO has a lengthy definition that includes 'accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment and broad-based participation'.[2] Taking from the world of corporate governance, we can identify two aspects of governance: performance (ensuring that whatever is being 'governed' performs in line with certain chosen objectives) and conformance (managing risks and compliance with relevant rules and norms).[3]

Effective digital governance results in greater economic benefits, enhanced security and risk management, and a digital arena that is consistent with and reinforces societal values. From an economic perspective, governance needs to enable technological innovation and entrepreneurialism, while protecting consumer rights and addressing issues of corporate market power that flow from the network and information structures often found in technology sectors. From a security perspective, governance needs to address issues of resilience (e.g., to cyberattacks from both state and non-state actors) and issues of external dependence (e.g., reliance on third parties for critical supplies or technologies). And from a values perspective, governance needs to both protect individual and community rights and support online discourse in a way consistent with a country's values.

Geopolitics inevitably shapes how such digital governance will evolve at the global rather than national level. The combination of technology and geopolitics is rarely out of today's headlines – be it 5G, semiconductors, the role of social media, AI or cyberattacks.

In March 2021, the UK published its Integrated Review of Security, Defence, Development and Foreign Policy.[4] This identified technology and shifts in global governance as two of the most important issues facing the UK. It noted that the "nature and distribution of global power is changing"; that "there are geopolitical and geo-economic shifts to China and the Indo-Pacific"; and that there is intensified "systemic competition between state and non-state actors". "Science and Technology will bring enormous benefits, but also be an arena of intensifying systemic competition". "There will be a growing contest – in which non-state actors will play an important role – to shape new rules, norms and standards and control access to shared resources such as space". For the UK, the Review identifies the ambitions of "sustaining strategic advantage through science and technology"; "shaping the open international order of the future"; and being a "responsible, democratic cyber power".

The US and China are at the centre of the debate on technology and global governance. Each are massive economies with their own giant technology companies and markedly different systems of government. In 2018, former Google CEO, Eric Schmidt, talked of the splitting into separate US- and China-led systems.[5] While the definition of such a 'splinternet' is unclear, some observers argue that it is already here.[6] Meanwhile in Europe, the EU – for the most part lacking its own large technology companies – seeks to position itself as a leader in digital regulation, distinct from the US and China.

---

1 https://dictionary.cambridge.org/dictionary/english/governance
2 http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance
3 https://knowledge.wharton.upenn.edu/article/corporate-boards-should-focus-on-performance-not-conformance/
4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf
5 https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html
6 https://techcrunch.com/2019/03/13/the-splinternet-is-already-here/

It has followed its GDPR law[7] on data protection with a new proposed framework for AI regulation.[8] Other countries face similar challenges of governance design. A recent article described Australia as "largely comfortable being a data primary producer and algorithm importer" in the field of AI, noting "that is probably not a safe place for any nation that values its security".[9]

Amidst this national level activity and changing geopolitics, what then is the role for global governance and what shape might it take?

7 General Data Protection Regulation: https://gdpr.eu
8 https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
9 https://www.themandarin.com.au/140740-opinion-whoever-controls-the-algorithms-controls-the-world/

II. Rationales for global governance and different forms

To understand the role for global digital governance, it is helpful to explore the rationale and forms of global governance more broadly. In the absence of a world government, global governance refers to the set of institutions, processes, agreements, and laws that individual nations agree to and participate in with other nations. The purpose is to achieve outcomes that are in some sense better than those that countries can achieve acting alone. In the language of economics, this is expressed as the provision of 'global public goods', outcomes that are of benefit to all and which benefit from common or coordinated action.[10] These outcomes can again be categorized a little imperfectly into those supporting human prosperity (esp. economic); those that strengthen security against threats and risks of all kinds; and those that promote or enforce certain universal standards of behaviour or values.

Concretely, this can take a number of forms:

1) Institutions and agreements to address a common external challenge – such as climate change (UN, COP process) or global public health (WHO);
2) Institutions and agreements that determine and enforce 'rules of the game' between countries – to improve economic outcomes (international trade/WTO); or enhance stability and security (arms control treaties, nuclear Non-Proliferation Treaty); or to bring about minimum or aspirational universal standards and values (forced labour/ILO), human rights/UNHRC);
3) Support to lower-income economies, for ongoing socio-economic development (e.g. World Bank, FAO) and in times of crisis (e.g. IMF, FAO).

The most extreme manifestation of global governance requires the participation and agreement of all nations of the earth. Such an approach would restrict the phrase primarily to activities undertaken by UN agencies or the World Trade Organisation. While the UN has the virtue of broad membership, this very fact also conditions the pace and nature of actions that it can take. Trade negotiations via the WTO have also faltered in recent years in the wake of the failed 2011 Doha Round.

Global governance is more practically seen as the entire patchwork of different groupings that address these global challenges. Smaller groupings can have significant global impact. Previously, the OECD and G-7 economies were of particular note. The creation of the G-20 in 1999, and its strengthening after the 2008 global financial crisis, has been important step in building a more inclusive, yet still limited approach to global governance. There has since been a proliferation of groupings to tackle supranational issues. Moreover, in the area of security, the UN's role has always been limited in relation to the largest countries. During the Cold War, it was a structure of security alliances that engaged in mutual negotiations, treaties and other interactions that kept the peace.

10 Strictly, they would be non-excludable (it is costly/infeasible to exclude others from enjoying the benefits) and non-rival (consumption by one does not reduce the amount available to others), though the term is often used more loosely

III. The shifting context for global governance

With the rise of China and rapid growth of developing Asian economies, the structure of global governance established in the wake of the Second World War is in flux. Efforts to establish new mechanisms of global digital governance, a relatively unformed terrain, take place against this backdrop.

Following World War II, the western allies led the establishment of multilateral institutions, often called the 'rules-based order' or 'rules-based international system'. The word 'liberal' is sometimes placed right in front to make explicit the values on which the order is based. At its simplest, this world order had three main elements:

1) The UN and its associated agencies, with essentially all countries as members, however strong geopolitical disagreements between them;
2) The Bretton Woods financial institutions underpinning economic activity mainly between market economies and supporting economic development in lower-income economies;
3) A military alliance (NATO) to address security issues, subsequently matched by the Soviet-led creation of the Warsaw Pact, and a subsequent series of arms treaties between them. Notably on the economic side too, there was the parallel development of the European Economic Community (as originally named) and COMECON.

With the end of the Cold War, questions of security receded in importance.[11]
The Washington Consensus of market-based economics, increasing economic integration, free trade and capital flows spread globally, together with a trend of increasing democratization. Famously, Fukuyama declared 'The End of History', as ideological struggle was judged to have withered on the vine.

This has now changed. The economic rise of Asia and (in particular) China means that non-western countries want to propose and implement their own perspectives on the scope and form of global governance. For a long time, there was an implicit assumption that, as it grew richer, China would converge towards Western versions of liberal democracy and free markets. This has not happened: rather the distinctions in economic and governance models have grown sharper. This means more negotiation on what governance looks like and more resources committed by countries to advancing national positions. Both Presidents Biden and Xi talk frequently of their commitment to multilateralism and the rules-based order. But whose rules and whose order? Biden also talks of 'extreme competition' with China, of a competition between democracy and autocracy.[12] China talks too of how it defends the international order, citing China's position as one of the first UN signatories as the Republic of China. But China also argues that the countries of the world do not want a US-imposed order, rather they want a genuinely international one.[13]

For any issue, the fundamental choices on the architecture of global governance are the same:

1) Agree to a single, global approach

   or

   Fail to agree and have separate, competing approaches (or none at all);
2) Recognise that agreeing on a single approach means compromise and consensus by all major parties

   or

11 Concerns switched rather to rogue states ('Axis of Evil') and terrorist attacks by non-state actors
12 https://www.theguardian.com/commentisfree/2021/may/02/america-has-woken-up-to-the-threat-posed-by-china-it-may-already-be-too-late
13 https://news.cgtn.com/news/2020-08-05/Wang-Yi-International-order-faces-challenge-of-unilateral-bullying-SIcZ31LCVy/index.html

Acceptance of one dominant perspective (which may be a performative acceptance that effectively ignores what has been agreed);

3) And that, where there are several competing approaches ('alliances', 'spheres of influence', 'regional blocs'?), the issue then arises as to how such competition is managed (if at all) and how are overlaps and disputes managed.

The greater divergence, competition and assertion of national autonomy between countries in today's world make agreement and compromise on a single approach more difficult in all but a few circumstances. China's emergence as a major global power – and the EU's ambitions to carve out a position distinct from either the US or China – makes the acceptance of a single dominant perspective less likely too.

In organisation design theory, when cultures and ways of operating differ widely, organizational structures typically separate rather than integrate. Carefully designed mechanisms then bring the different parts together where needed. Global governance appears headed in the same direction. To return to the UK's Integrated Review:" those parts of the international architecture where multilateral cooperation adds value, such as the International Financial Institutions, are more likely to thrive. Conversely, where multilateral approaches are blocked, nations will likely caucus in smaller, regional or like-minded groups."[14]

14 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf, p. 28

IV. Global digital governance: Evolution, benefits and challenges

Against this backdrop, leaders around the world face the task of shaping global digital governance. To date, digital governance can be described as, at best, nascent – and, where it exists, technically-focused and US-centric.
The future certainly promises much more extensive governance at national level, with less certainty about the global dimension.
This governance will need to go far beyond technical aspects to address issues of economics, security, and values. Now is the time for the substantial investment of policy-making resources, leadership time and political will to put in place the right governance design across all walks of life.

Digital governance has to date been mainly technical in nature, with standards developed and agreed by standards development organisations (SDOs) at national and international level. According to one paper, "more than two hundred (SDOs) are developing standards for information and communication technologies (ICT)",[15] many private sector-led. Key for 5G standards, are the International Telecommunications Union (ITU), a UN agency and 3GPP, a private sector-led entity, operating by consensus.[16] While corporate and national interests have always played a role, discussion has focused primarily on the technically appropriate solution, while maintaining the benefits of common standards. The 3GPP argues that "its consensus-based and transparent approach, procedural rules, and elected leadership promote regional balance and 'has been successful in preventing the fragmentation of the GSM (and its successors) ecosystem.'"[17]

Despite its origins as a US Department of Defense initiative, the internet rapidly evolved to a multi-stakeholder model of governance, as the US government "lost interest".[18] Non-profit organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) continue to play a key technically focused role. Alongside this technical focus, early internet pioneers espoused the important of a 'free and open' internet, born out of American libertarian ideals, with little or no government interference.[19]

Finally, the pace of technological innovation means that, in many areas, there is a simple absence of governance at the national level, before considering the global level. One report notes that the US "has no unified federal approach to privacy but instead an array of sectoral rules, state-level legal frameworks and private-sector practices".[20]

The internet is no longer US-centric. Benedict Evans, an independent technology analyst, has written of 'the end of the American internet',[21] with 80-90% of smartphone users outside the US. In 5G, semiconductors and AI, much of the innovation and manufacturing capability is now outside the US. National governments around the world are seeking to regulate the digital arena and the companies within it in their own way. Again, in the words of Benedict Evans, "technology is becoming a regulated industry."[22]

The aims of digital governance are analogous to those of governance in the non-digital world. It manifests itself in institutions, processes, and regulations that:

15 https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781119043492.oth
16 https://www.wiley.law/assets/htmldocuments/Tech-Standards.pdf
17 https://www.wiley.law/assets/htmldocuments/Tech-Standards.pdf
18 https://www.gppi.net/media/Internet-Governance-Past-Present-and-Future.pdf
19 https://www.gppi.net/2019/03/12/the-web-at-30
20 https://www.csis.org/analysis/governing-data-asia-pacific
21 https://www.ben-evans.com/benedictevans/2020/10/3/the-end-of-the-american-internet
22 https://www.ben-evans.com/benedictevans/2020/12/03/the-regulators-puzzle

– Support economic prosperity: including reaping the benefits of common standards; effective anti-trust, competition and taxation policies; and international trade and investment agreements that promote fair and open trade;
– Enhance security and resilience by protecting against cyberattacks; avoiding dependence on third parties for critical resources; and putting in place confidence-building measures that maintain stability and share understanding with relevant third parties;
– Protect societal values in terms of privacy, information rights, the use of technology in decision-making, social discourse and debate;
– Support socio-economic development in lower-income economies through strengthening their own digital governance.

What remains unclear is where the benefits of a common global approach outweigh the challenges. The increasing integration of trade, investment, knowledge and people flows in the world economy has enabled much of the technological innovation and growth in prosperity of the past few decades. Now, however, the direction is one of 'deglobalisation' driven by different economic development models, concerns on national security and different societal values and systems of government. With the emergence of globally distributed, tightly integrated product value chains, common standards and a high degree of interdependence between countries, little attention was paid to the nationality of individual suppliers. This has now changed markedly – especially in the area of critical technologies such as 5G and semiconductors and in the whole arena of data. Globally, much of the policy debate now focuses on the risks of dependence rather than the benefits of interdependence.

We can consider what this all means for the shape and nature of global digital governance by considering five aspects separately:

1. Standards and shared infrastructure
2. Industrial policy, trade and foreign investment, and corporate regulation
3. Digital trade: data flows, online discourse and algorithms
4. Defence and security
5. 'Rest of the World' and global development.

V. Standards and shared infrastructure

The benefits of maintaining uniform global standards based on technical criteria are significant on both the supply and demand side. On the supply side, such global standards provide a focal point for continued innovation and improvement. Manufacturers can focus productivity efforts on a single platform, driving costs down while avoiding the complexity costs of developing separate product lines for markets with differing standards. From the customer perspective, shared standards eliminate the need to judge which standard will fare better over time: as, for example, was the case in the VHS vs Betamax format wars in consumer video recorders in the 1970s and 80s.[23]
Single standards allow for interoperability in global businesses, bringing both convenience and cost benefits, and are a significant convenience in a world of mobility.

The wider benefits of standards

But standards are rarely purely technical in their impact. Whether common standards win out depends how large are the economics, security and values implications of particular technical choices.

Standards generate an economic return to those who own the patents underlying the standards, a return on successful innovation efforts.
But the real significance is that those who set standards are able to shape future development. The specific standards chosen can shape a sector's competitive structure and industry economics: "Third-tier companies make products; second-tier companies make technology; and first-tier companies make standards".[24]

Across many fields, China has announced ambitions to set standards domestically and then have these serve as international standards under its China Standards 2035 initiative.[25, 26] This includes resourcing and structuring its own standards organisations in ways that mirror the structure of international organisations and so enable China to state its own case more effectively.[27] For China's plans to succeed, however, the reality is, is that all parties would need to agree that these standards are indeed mutually beneficial.[28] Where the focus is on tangible technical benefits, this is plausible. The more that proposed standards raise issues of economic competitiveness, security and even values, the more attractive it is to accept a separation into competing standards, if a mutually acceptable consensus cannot be reached.

Different technical standards also have a values dimension. More precisely, they enable or hinder certain actions that may favour or undermine certain societal values.

In the realm of cryptocurrencies, Bitcoin has found favour for the anonymous, decentralized, yet trustworthy nature of blockchain architecture. Central banks are now planning their own CBDCs (central bank digital currencies) where different security and stability considerations are at play. China is at the forefront with its DC/EP (digital currency/electronic payment) initiative.
Rather than being anonymous and decentralised, this e-renminbi has a centralized architecture. This raises the technical possibility of identifying each payment made by each individual, yet in practice China's central bank is employing a philosophy of 'managed anonymity' whereby small-value payments are anonymous. Some of form of identification will be needed in

23 https://medium.com/swlh/vhs-vs-beta-the-story-of-the-original-format-war-a5fd84668748
24 https://saiscsr.org/2019/10/29/setting-a-new-standard-implications-of-chinas-emerging-standardization-strategy/
25 https://merics.org/en/analysis/chinese-tech-standards-put-screws-european-companies
26 https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/technical-standardisation-china-and-the-future-international-order.pdf
27 https://macropolo.org/analysis/standards-bearer-a-case-study-of-chinas-leadership-in-autonomous-vehicle-standards/
28 https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype

all countries,[29] yet the debate on privacy and the appropriate role of government will differ between countries. A single global standard that secures support is unlikely.

Reaching agreement on next-generation internet standards

More fundamental still is the architecture and associated governance of the internet. The ITU has issued papers discussing the so-called New IP (Internet Protocol), the technical architecture of a next-generation internet design for 2030, with particular input from the Chinese government and leading Chinese companies.[30]

Internet governance today is "a congeries of systems, protocols, standards, hardware and organizations. It encompasses the domain name system (DNS), information intermediaries, security systems, exchange points, autonomous systems, internet service providers (ISPs), registers, databases and standards bodies — some with national standing, some (often in the United States) with global reach, and others of international standing — as well as some public bodies, some private companies and some non-profit organizations".[31] In short, it is a multi-stakeholder model of governance.

China, together with Russia and others, has instead argued for an inter-governmental model of governance. The new Chinese-advanced design proposal is centralized and top-down. The stronger role that it would allow to national governments fits with China's stance on cyber-sovereignty, first advanced in a 2010 Internet White Paper:[32, 33] unwanted influence in a country's 'information space' should be banned.[34]

Discussions on the New IP are at an early stage. How the very structure of the internet evolves will rest on more than technical considerations. The defining issue remains whether countries can agree on a single best architecture for the next-generation internet, all things considered. Or whether the compromises involved are deemed too great, so that two parallel architectures emerge, each under their own governance structure. At the worldwide level, the questions then centre on how these competing structures develop and how users access both: Does each country choose an architecture or do both co-exist in a country? Do the different network architectures have implications for internet access or remain hidden 'plumbing'? Can a single device access both or are different devices needed?

Physical infrastructure – shared or separate?

Common standards are a form of shared global infrastructure. Global physical infrastructure also underpins the availability of digital access worldwide. The desire for national control and reduced dependence on others is already leading to separate, competing networks.

To avoid reliance on the US government's GPS system,[35] the EU developed its own system (Galileo[36]) as did China (Beidou[37]). Elon Musk's Starlink is leading the development of a global satellite internet system. China has announced its own plan for satellite internet and identified satellite internet as a priority technology for development.[38]

Yet 95% of international internet data flows are carried by subsea cables.[39] One recent paper noted that "China is emerging is as a leading provider and owner of subsea cables" and called

29 https://www.ft.com/content/88f47c48-97fe-4df3-854e-0d404a3a5f9a
30 https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Documents/Internet_2030%20.pdf
31 https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf
32 https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf
33 https://www.gppi.net/media/Internet-Governance-Past-Present-and-Future.pdf
34 https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/
35 https://www.gps.gov/systems/gps/
36 https://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo
37 https://www.bbc.co.uk/news/technology-45471959
38 https://spacenews.com/china-is-developing-plans-for-a-13000-satellite-communications-megaconstellation/
39 p. 3: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ

for “protecting US centrality in subsea networks”.[40] While the main cause of faults in subsea cables are shipping and fishing activities, there have been cases of cables being cut. In 2008, such cuts limited the US’s ability to conduct drone flights in Iraq.[41] In an era of increased geopolitical competition and tensions, all countries will have interests in the resilience and security of these cables. National measures will be a part of this but finding governance mechanisms to address concerns and limit duplicate investment in cables has great merit.

40 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ

41 p. 14: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ

VI. Industrial policy, trade and foreign investment, and corporate regulation

It is in the area of trade and investment rather than standards that China's technological rise has had the greatest policy impact to date. Interventionist industrial policy and the creation of national champions are back on the agenda in the West. This follows a period of market-based liberalization of trade and industrial policy, with decisions made on an essentially commercial basis. Limits on state aid, government subsidies and support to state-owned enterprises together with open procurement standards have been important elements of global trade negotiations. Now, major economies are increasing state aid and emphasizing supplier nationality in procurement decisions. The challenge for global governance is how to maintain the benefits of economic integration through trade and investment flows in this new environment.

The return of industrial policy

Governments see leadership in 5G (and subsequently 6G) as critical to next-generation productivity improvements across all sectors of the economy, in particular through the enablement of IoT (Internet of things) applications. Beyond that, they see the deployment of AI, quantum computing and robotics as key elements of future prosperity, competitiveness and, ultimately, job creation (despite the directly labour-reducing impact of some technologies). China's Made in China 2025 policy identified 10 priority sectors for technological development including robotics and new materials.[42] Increasingly, the US and Europe state the need for their own government-guided efforts in technology as a national imperative. The debate in US has parallels with that about Japanese technological prowess in the 1980s and 90s. The UK plans to establish ARIA, the Advanced Research and Invention Agency[43] as a stimulus for further innovation.

Beyond the economic perspective, security concerns – both real and perceived – loom large. The spectre of national security immediately shifts the discussion to national self-reliance and working with 'like-minded' partners and away from global integration and interdependence.

There are three distinct aspects to the national security question.

First, if leadership in new technologies is fundamental to economic prosperity, then there is a potential security risk when a foreign country is the main supplier of such technologies and able to restrict access. As result, countries are reviewing their technology supply chains to identify potential dependencies on overseas supply. Countries are also strengthening the investment screening of technology acquisitions by foreign companies in order to keep control of capabilities. In the UK, for example, the National Security & Investment Bill determines approval requirements for foreign acquisitions of UK companies in certain key technologies.

Second, as digital technology becomes increasingly pervasive across daily life, so vulnerabilities to cyberattacks increase. The UK has identified 13 sectors of critical national infrastructure (CNI)[44] including emergency services, civil nuclear, water and transportation, all of which could be the target of cyberattacks. One important question here is whether using foreign equipment leads to less resilient systems or whether risks are similar whatever country's products are used.

Finally, technologies such as AI, robotics and quantum computing are themselves critical to

42 https://merics.org/sites/default/files/2020-04/Made%20in%20China%202025.pdf
43 https://www.gov.uk/government/publications/advanced-research-and-invention-agency-aria-statement-of-policy-intent/advanced-research-and-invention-agency-aria-policy-statement
44 https://www.cpni.gov.uk/critical-national-infrastructure-0

the future development of military and defence capabilities. Developing superior offensive and defensive capabilities is a critical element of national security. This reinforces the desire to have proprietary capabilities and limit foreign acquisitions. Former Google CEO, Eric Schmidt, chaired the National Security Commission on Artificial Intelligence in the US.[45] The final report presented an "integrated national strategy to reorganise the government, reorient the nation and rally our closest allies to defend and compete in the coming era of AI-accelerated competition and conflict." This framing is not so different to that of a Chinese government announcement.

Implications for global trade and investment agreements

This all creates an environment of increasing protectionism and an unravelling or reshaping of the global and regional value chains that have provided economic benefits and proven to be resilient. It makes new global agreements on trade and investment liberalization even more difficult.

These trends highlight the need for renewed negotiations that seek to preserve and restore interdependence in parts of the technology chain. Such agreements are easiest between countries that are 'like-minded' or, more specifically, see one another as reliable trading partners and not (potential) security risks.
As the US narrative of 'extreme competition' with China has strengthened, so the G-7 grouping of large, democratic economies has regained significance. This comes after a period of greater emphasis on co-operation in the broader, more diverse G-20 grouping following the 2008 financial crisis. The June 2021 G7 summit in Cornwall saw an informal expansion to a D-11 gathering where Australia, India, South Africa and South Korea joined. A T-10 or -11 (focused on technology) could be a natural development. The US and EU have also launched the US-EU Trade and Technology Council to address issues of technology trade and standards.[46] In 5G, there have been various informal discussions with Korea, Japan, the UK, US and EU on how to create a competitive 5G ecosystem. Expanding the scope of the Five Eyes intelligence agreement to include a technology component has also been mooted. All are outline agreements or draft concepts rather than specific measures at this stage. They do though point to a mingling of industrial policy and values in the approach to multilateral agreements.

More broadly, with the resurgence of industrial policy in key technologies, there will be value in trade negotiations that revisit the terms for state aid and domestic procurement. While countries will invoke national security arguments, there is a need to retain as much of a level playing field between domestic and foreign competitors as possible in order to minimize the economic losses from increasing protectionism.

Regulating the corporate behaviour of Big Tech

Alongside this security-driven perspective, there remain important questions of how to regulate technology companies and what role, if any, there is for global governance.
This includes questions of anti-trust, information usage, compliance and digital taxation.

The challenge is made somewhat simpler by the clear separation between the Chinese and western internet ecosystems. China has its so-called BAT[47] companies and the US has its FAANG[48] companies. Apple is the one company that straddles both worlds in a significant way. For China, the question is essentially one of domestic policy and China has made significant moves to address anti-competitive practices and non-compliance by its largest tech companies.[49]

45 https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf
46 https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/
47 BAT = Baidu, Alibaba, Tencent. More accurately today: Alibaba, Bytedance, JD, Meituan, Pinduoduo, Tencent
48 FAANG = Facebook, Amazon, Apple, Netflix, Google (Alphabet)
49 https://www.brookings.edu/blog/techtank/2021/04/16/the-chinese-government-embraces-tech-industry-competition/

The challenge remains of transatlantic agreement between the US and EU, which have developed their own independent anti-trust regimes as well as markedly different approaches to data protection. The G7 and US-EU initiatives again highlight the mutual desire to reach agreement but agreeing specific measures may prove tougher. With the new Biden administration, there has been sudden and significant progress in the area of digital taxation as part of the US-led initiative on global corporate taxation.[50] The focus on first reaching agreement within the G7 countries has led to progress, but left many countries dissatisfied that the solution does not provide them with a fair share of tax revenue. Other discussions continue about an OECD-level approach and an UN-led initiative.[51]

One analogy for the role of global governance is the development of international financial regulation after the 2008 financial crisis. While the crisis reinforced the critical role of national-level regulation in the financial sector, it also led to the creation of the Financial Stability Board (FSB)[52] at a global level. Established by the G-20, it therefore included a much broader range of economies than the G-7, including China.

The FSB organizes its work around three Standing Committees: those on the Assessment of Vulnerabilities; on Supervisory and Regulatory Cooperation; and on Standards Implementation. Additionally, the FSB has led work identifying those financial institutions that are systemically important and pose particular risks. These are the G-SIFI's, global systemically important financial institutions and G-SIBs (banks).[53] As of November 2020, there were 30 G-SIBs, notably including US, Chinese, European and Japanese institutions.[54] The Basel Committee on Banking Supervision (BCBS) also continues play an important role as 'the major global standard setter for the prudential regulation of banks',[55] covering 28 jurisdictions, again including the US and China.

Analogous structures in the internet arena may provide a mechanism both for international coordination on managing the impact of Big Tech companies (e.g. antitrust, use of information, compliance, moderation of social media debate) and of the resilience of the internet itself. The G-SIB concept provides a precedent for identifying critical institutions at a global level and determining what risks then need to be managed.

50 https://www.bbc.co.uk/news/world-57368247
51 https://www.ft.com/content/9f8304c5-5aad-4064-9218-54070981fb4d
52 https://www.fsb.org
53 https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/post-2008-financial-crisis-reforms/ending-too-big-to-fail/global-systemically-important-financial-institutions-g-sifis/
54 https://www.fsb.org/wp-content/uploads/P111120.pdf
55 https://www.bis.org/bcbs/index.htm?m=3%7C14%7C625

VII. Digital trade: data flows, online discourse and algorithms

Trade agreements have always concentrated more on trade in goods than services. They need upgrading and adapting to take account of the digital economy, data flows and services. In part, this simply reflects the need for trade agreements to catch up with innovation. However, data protectionism is also on the rise, driven again by concerns of economics, security and values. These concerns will shape the potential role for international agreements and governance. Solutions will require granularity about exactly what 'data' means in each situation.

Data from a geopolitical perspective

'Data' is seen increasingly as a source of economic competitive advantage. When comparing the US and China in the field of AI, China is often judged to have an advantage based on the sheer scale of data generated by its 1.4 billion population. The issue is more complicated: Matt Sheehan of the Paulson Institute identifies five key dimensions for a deeper comparison of relative competitive positions in data.[56] But, in the context of increasing economic nationalism, the topic of 'data exports' hits an economic nerve.

There is a similar argument in terms of security. Once data has moved to another country, there is a suspicion that governments may then use it for other purposes. At a time of mutual mistrust, the conceptual potential for misuse is enough to justify action. Differences in societal values and how these are expressed in national legislation also play an important role in regulation of all kinds. These differences go beyond choices on the regulation of data privacy and ownership. They also include the nature and regulation of social media discourse. What qualifies as 'hate speech' or 'fake news'? Which actions are censorship, and which are valid interventions? How are individual wishes for expression and privacy weighed against the demands – real or perceived – of national security?

Societies vary widely in their answers to these questions. Governments, both authoritarian and democratic, take different views on what should be permitted and, indeed, how this regulation should occur. The EU approach to consumer data privacy through GDPR is significantly more restrictive than that of the US, which gives fewer rights to the consumer and more to business.

Liberalising data flows

Digital trade and cross-border data flows play an increasingly important role in economic activity. Liberalization of cross-border data flows brings economic benefits: data can be more easily aggregated and analysed across borders for customer and business insights; data centre networks can be optimised based on economics rather than the need for a presence in each country; and the administrative efforts required to comply with data localisation and transfer requirements can be avoided. International agreement helps eliminate the question posed by Benedict Evans, an independent technology analyst: "If I like a photo posted on Instagram by a friend in New York, where does the EU want the data to be stored?"[57]

Such agreement rests, of course, on mutual agreement that data is being handled in ways consistent with a country's choices on consumer data protection rights and without posing risks to national security – again as defined by each country. Agreeing terms between widely different societies and regulatory environments is a tough challenge. Indeed, restrictions are increasing.[58, 59]

---

56 https://macropolo.org/ai-data-us-china/?rp=m
57 https://twitter.com/benedictevans?s=11
58 https://www.newamerica.org/cybersecurity-initiative/reports/global-data-governance/theme-1-growing-restrictions-on-free-data-flows/
59 https://asia.nikkei.com/Opinion/Incoherent-regulations-will-devastate-Asia-s-digital-economy

With increasing geopolitical competition, it will be difficult to secure global agreement on rules of the game that support digital trade and data flows. WTO efforts to progress trade talks had already faltered on simpler matters and before the US-China trade tensions. While a single global effort to resolve these questions would be desirable, prospects for immediate progress appear limited.

As in other trade discussions, groupings of like-minded countries, often regionally, are better positioned to reach agreement. Recently, it is Asia-Pacific that has made the most progress, including on questions of digital trade. The region is now home to two new trade agreements, CPTTP[60] and RCEP.[61] In simple terms, RCEP is a looser arrangement, requiring less opening and granting more discretion in the application of agreed rules. Each has a digital chapter, with CPTTP significantly more liberalised than RCEP in areas such as data flows. DEPA, the Digital Economy Partnership Agreement, signed by Singapore, New Zealand and Chile goes further.

China has joined RCEP, applied to join CPTPP and stated that it wishes to join DEPA. The US is in none of these agreements. One report made a strong case for the Biden administration to take the lead in securing agreement on data governance across the Asia-Pacific[62] as part of its engagement in the Indo-Pacific. The report noted, however, that the absence of a US federal (vs state-led) approach to data governance was a hindrance.

There are in fact a myriad of bilateral and plurilateral initiatives addressing different aspects of international data governance. What is lacking – among the G-7 economies and between the EU and the US – is some form of mutual recognition or the carving out some core, standard elements that reduce the costs of dealing with multiple standards.[63] The US-EU attempts to do so with the EU-US Privacy Shield Framework were rejected by the Court of Justice of the European Union[64] though both sides have restated their commitment to find a resolution.[65]

It may be possible to reach agreement with more countries on certain, narrowly defined, types of 'data', for very specific reasons. Combating online child pornography would be one such example. Where societies are more similar, or more 'like-minded', then the scope of discussion can be broader. This may open up a path for, say, the world's major democracies to explore how online debate should be moderated or on how to oversee the actions of major US tech companies in moderating debate.

Algorithms and AI

New technologies – in particular, AI and the increased use of algorithms in decision-making increase both the importance and the challenges of reaching international agreement.

At its simplest, AI reaches a myriad of decisions by combining large amounts of data and algorithms that analyse the data. Many such algorithms inherently incorporate value judgments, implicitly or explicitly. Even the decision to build a certain AI capability may entail a value judgment. Famously, self-driving cars need to determine how to weigh the certain death of the driver against a limited possibility of death for pedestrians, either old or young.

How to regulate such matters is a subject of debate globally. With facial recognition technologies, for example, where does usage bring benefits through increased convenience or enhanced safety and crime prevention and where is it an unwarranted invasion of privacy or used to suppress dissent.

---

60 Comprehensive Agreement for Trans-Pacific Partnership: Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam. CPTPP came about after the US withdrew from negotiations on the TPP (Trans-Pacific Partnership)

61 Regional Comprehensive Economic Partnership: ASEAN + China, South Korea, Japan, Australia and New Zealand

62 https://www.csis.org/analysis/governing-data-asia-pacific

63 https://www.csis.org/analysis/advancing-data-governance-g7

64 https://www.euractiv.com/section/data-protection/opinion/eu-us-in-collision-course-on-privacy/

65 https://www.reuters.com/technology/more-safeguards-revamped-eu-data-transfer-tools-eu-justice-chief-says-2021-06-02/

Yet a unified global approach appears highly unlikely. Societal norms vary widely. In cases of national security, countries will retain the right to use such technology – but will differ on what constitutes 'national security'. Additionally, as with data privacy, countries will reach different views on the balance of regulation between encouraging business-led AI innovation and protecting consumer rights. Such differences lead then to the same questions of cross-border flows: what happens when data is sent to an algorithm in another jurisdiction with the result sent back? Or what inspections need to take place to allow the 'import' of an algorithm? There will still be a need and great value in agreeing rules by which such 'trade' can happen.

VIII. Defence and security

Security and resilience against threats and appear repeatedly in considerations of digital governance. They provide the rationale for increasingly nation-based actions and closer cooperation with like-minded countries, while 'decoupling' or separating from others. Beyond the risks of economic dependency considered previously, there are the risks of cyberattacks and the role of technology in warfare itself. Global governance mechanisms that can address such concerns need to start with consideration of the nature and source of such threats, real and potential.

The overall landscape of cyberattacks is complicated. Many different actors operate with different motives and at different levels of sophistication.[66] The perpetrators are a mixture of governments and non-state actors (criminal gangs and terrorists), with the latter both operating on their own account and, at times, with implicit or explicit support of governments. While many, if not most, protective measures against cyberattacks need to be taken at the level of individual institutions and national governments, there is scope for international cooperation. Distinguishing between state and non-state actors, although sometimes difficult, helps clarify approaches to international governance at a first approximation.

Criminal and anti-terror-like activity

Where non-state actors are effectively operating independent of any governmental support, the approach to international governance can be similar to that of international criminal or anti-terrorism activity. The DarkSide gang behind the ransomware attack on the US Colonial Pipeline was quick to announce that it was purely seeking financial gain: "Our goal is to make money and not create problems for society."[67] As DarkSide is based in Russia, the US has raised the attack as essentially a law enforcement question with Russian government where Russia should act.[68]

As with Interpol, there is value in sharing information on such attacks and an expectation that countries act against criminals operating on their own soil. There is scope to reach agreement both on norms on paying ransom demands (as in paying terrorists) and in pursuing and closing down the criminal networks involved.

This is significantly less effective when the non-state actors operate with the connivance of the government or rule of law is not effective. A non-cyber parallel here would be Al-Qaeda's presence in Afghanistan and Pakistan.

State-based attacks

To the extent that governments are involved, the closest analogy is that of traditional military and intelligence matters. Countries build capabilities to protect against cyberattacks, have capabilities to launch attacks themselves, and act in ways to deter attacks. They work closely with certain partners or allies. This provides mutual support in protecting against what they see as external threats. They can also continue to reap the benefits of economic interdependence without undue concerns on security.

Other countries are classified implicitly or explicitly as 'adversaries'. Engagement with these countries takes the form of agreements that reduce tensions and increase stability. This can come through improved understanding of mutual intentions and 'red-lines'; through a definition of 'rules of the game' or 'rules of engagement'; and through confidence-building measures such as personnel exchanges, mutual monitoring and inspection (or use of third parties). Such approaches between the US and Soviet Union characterized the era of détente

66 https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf
67 https://www.bbc.co.uk/news/business-57050690
68 https://www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html

and maintained stability through periods of great tension. SALT and START arms control negotiations addressed the specifics of offensive and defensive missile capability in, at times, arcane detail.

This framing is appropriate to the issue of potential attacks that damage critical infrastructure: alliances between like-minded countries and structured engagement with potential adversaries to reduce tensions. There are though significant differences today from the Cold War period. Tensions between the US and China or Russia are much less entrenched and focused. While there is a broad range of potential attacks on critical infrastructure that either side could unleash, describing them and then agreeing and monitoring rules of engagement and 'red lines' is a much knottier problem.

In fact, beyond ransomware attacks, it can be difficult to categorise the nature of cyberattacks and so hard to determine appropriate responses or develop rules of the game.[69] For example, if a government launched a massive cyberattack that disabled critical infrastructure, then a military response may be justified and appropriate. But cyberattacks almost always fall short of this and the appropriate response is ambiguous.

Moreover, cyberattacks that seek to gain information (rather than inflict damage) are essentially equivalent to espionage.[70] This has long been accepted as something that happens between countries, but where each does its best to protect itself. The Solar Winds attack[71] showed, however, that even this categorisation is not clear-cut. The same cyberattacks that harvest information may create the potential to inflict damage (e.g. by disabling power systems) at a later date. In the physical world, planting a bomb in a nuclear power station but not yet detonating it is a markedly different act from stealing the power station plans.[72]

The rise of online disinformation campaigns on social media complicates the matter further. It is messy to disentangle non-state action from state action (either direct or through non-state actors) to separate 'fake news' from legitimate but alternative interpretations. To shape online discourse in a country, 'bot farms' create fake social media accounts on a large scale to both post messages and boost the messages of others.[73]

All this ambiguity coupled with the extreme costs of potential misunderstanding reinforce the benefit of international engagement that would develop an approach to international governance of the most dangerous cyberattacks. The aim would be to seek to agree rules of the game (or at least a description of what the 'game' is) between – primarily – the major players in this sphere in particular the US, key European countries, China and Russia. Work under the auspices of the UN has made progress in describing the issues.[74] But this is quite different from securing and enforcing agreements between the major actors.

The competitive and confidential nature of cyber offensive and defensive capabilities hinders significant information-sharing between any but the closest international partners in identifying the sources of specific attacks.

Impact of new technologies: AI, quantum computing and robotics

New technologies such as AI, quantum computing and robotics bring additional considerations for cyberwarfare. These technologies may make military decision-making faster, unhackable and independent of human input. One report suggests that the Pentagon is increasingly convinced that machines use

69 https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf
70 https://www.iiss.org/blogs/survival-blog/2021/04/lessons-of-the-solarwinds-hack
71 https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/
72 https://www.lawfareblog.com/cyber-deterrence-brexit-analogy
73 https://jamestown.org/program/russian-bot-farms-the-new-old-challenge-to-ukraines-national-security/
74 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

weapons more effectively than humans in complex situations.[75] Such automation of military capabilities also raises issues of ethics and values: the act of killing becomes increasingly detached from human involvement and intention. In short-hand, what are the limits and norms for the use of 'robot-soldiers'? Can a computer decide to launch a large-scale missile attack? Famously, in 1983 Stanislav Petrov ignored what he deemed to be false computer alarms of a US nuclear launch against the Soviet Union. So, the Soviet Union did not retaliate against the indeed-false reports, avoiding nuclear war.[76] Would a fully automated process be programmed to effectively ignore itself in the same way? In the area of disinformation and 'fake news', the rapid improvements in deep-fake video technology will soon make possible fake videos of government leaders that are indistinguishable from reality.

A Brookings report has called for the negotiation of global treaties on artificial intelligence.[77] Several analogies are relevant: to the deployment of new missile systems by the US and USSR in the Cold War; to agreements on the non-proliferation of nuclear weapons technology; and to worldwide bans on the use of chemical and biological weapons on moral grounds. The Chemical Weapons Convention signed in 1993,[78] with now 195 signatories, "aims to eliminate an entire category of weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons".

Similar regulation of AI poses major challenges. First, AI itself is a broad-brush concept. Agreements would need to distinguish between more tightly defined applications, use-cases and technologies. Some agreements might most usefully be bilateral or trilateral; others might be global in scope. Secondly, the level of AI capability is itself a matter of competition between different countries. It is also hard to assess and inspect from the outside and such inspection would itself require a high level of capability. The challenges here are greater than those involved in controlling certain categories of nuclear weapon, or even in the inspection of nuclear power facilities to determine whether weapons-grade materials development is underway. Thirdly, preventing the proliferation of certain technologies is destined to fail given the ease of transmission: The Wombo.ai app[79] already provides the beginnings of deep fake video-making on a smartphone.

All the challenges do not mean that attempting to define common rules, norms and monitoring is not worth the effort. Engagement and discussion are particularly valuable in new, undefined areas of competition and discovery, where countries may not fully grasp the issues and risks involved. A good starting point for discussion between the US and China (and other major countries) would be to agree the very terms of engagement ('talks about talks'). This would set out a typology of issues potentially raised by AI and other technologies. Parties involved could then determine whether and where there is shared agreement that the benefits and risks of having 'rules of the games' outweigh the benefits and risks of competitive, unconstrained development. Such discussion provides a shared view of the landscape of emerging risks. It may also result in a small number of narrowly defined areas where co-operative agreement can be reached.

75 https://www.wired.com/story/pentagon-inches-toward-letting-ai-control-weapons/
76 https://www.bbc.co.uk/news/world-europe-24280831
77 https://www.brookings.edu/blog/techtank/2021/03/24/it-is-time-to-negotiate-global-treaties-on-artificial-intelligence/
78 https://www.opcw.org/chemical-weapons-convention
79 https://www.wombo.ai

IX. 'Rest of the world' and global development

China, the US and the EU account for only 28% of the world's population. These three geographies feature most frequently in discussions of digital governance, yet other countries face the same challenges. What the rest of the world? India stands out as a massive, lower-income economy that has its own technological strengths and has taken measures to restrict Chinese activities in 5G and apps such as TikTok.[80, 81]

So-called 'middle powers', smaller, higher-income countries, such as the UK, Australia and Japan, are actively working on all aspects of digital governance including international approaches across economics, security and values. Lower-income countries, however, generally face greater challenges. Efforts to support such countries in their socio-economic development and crisis response have long been a part of global governance.

From an economic perspective, technology infrastructure is now itself a critical part of a country's development needs. China has already adapted its approach, in large part through its Digital Silk Road, the digital manifestation of the broader Belt and Road Initiative. This brings Chinese tech companies (and their standards) to enable economic and social development, while also offering China's approach to security, information and online discourse.

Countries face similar challenges of how to moderate online discussion, preserve and strength political discourse, maintain and control information and protect against cyberattacks. While some are developing their own technology giants,[82] almost all face the challenge of how to deal with foreign tech giants operating in their countries.

The Washington Consensus approach to development currently offers little help here. Global development agencies and programs need to adapt accordingly. All countries need to protect themselves from cyberattacks by both state and non-state sources. As such they benefit from a global approach where this is feasible and from the sharing of basic cyber-defence capabilities. Based on experience and reports, they remain wary of the security aspects of any technology, whatever the national origin. But they also recognize the benefits of technology and prioritise having some, imperfect technology over none at all. The role here for global institutions is to sensitise governments in lower-income economies to the risks and to provide a better range of ways to mitigate them.

In the area of online discourse, governments are following the same path as larger, richer economies – increasing regulation of data and social media and insisting that Facebook and Twitter appoint local representatives to be responsible for compliance.[83] After a period of unrestricted online speech in many of these countries, the battle between free speech and censorship has moved online. In this sphere, at least, the trend is away from the 'open and free' origins of the internet towards the model of 'cyber-sovereignty' where each country governs its own information space.

Countries are best placed to make their own decisions on how they develop their national digital governance. Global institutions can provide technical assistance to help them make better choices by understanding the issues and options.

---

80 https://www.bbc.co.uk/news/business-56990236
81 https://economictimes.indiatimes.com/tech/technology/india-to-permanently-ban-59-chinese-apps-including-tiktok/articleshow/80451148.cms?from=mdr
82 Go-Jek (Indonesia); SEA and Grab (SE Asia); Mercado Libre (Latin America)
83 https://restofworld.org/2021/social-media-laws-twitter-facebook/

X. Conclusion and priorities for action: Creating a new governance patchwork

Technology's pervasive role in all aspects of life means that digital governance will be shaped by societal context. The role for such governance at the global level – extensive or limited – will reflect the realities of today's geopolitical environment. It will inevitably engage with issues of economic prosperity, national security and values as much as with technical specifications. For specific agreements or institutions to be global in scope, they will need to accommodate and find common ground between divergent perspectives – not just between the US and China, but also those of India, the EU and others. In many cases, this will be too difficult – at least, as a starting point. The current patchwork of country groupings covering different topics will get more complicated. In some areas, common global standards will remain; in others they will diverge. Such developments will at least partially resolve concerns of security and values, but risk jeopardising some of the economic benefits of common standards, liberalised trade and globally integrated knowledge flows.

Now is the time to invest time and attention into the specifics of governance, across the many areas that are new or have not been well-regulated to date. There is nothing preordained about the precise future shape and effectiveness of this digital governance patchwork. It is the choices and actions of leaders that will make the difference. The prize is to preserve the bulk of the benefits of global trade, shared scientific research endeavours and common standards, while addressing concerns on security, risks and values. Individual governments are active in defining and implementing digital governance at home. In parallel, they need to engage in similar efforts internationally. This will, by necessity, mean building on ever-shifting national structures and taking account of new technological opportunities and challenges as they arise.

The breadth, diversity and fluidity of issues calls for a multi-pronged approach that makes use of both existing and new institutional structures:

1) Match the resourcing of initiatives in global digital governance to the scale and nature of the challenge. Technology's impact on society is a new, relatively unregulated domain, where many important governance questions have yet to be addressed. The economic and demographic heft of Asia and, in particular, China means that shaping global standards and governance has become a more competitive game. Countries need to make their best arguments for what standards and governance design make sense where. Efforts to maintain the benefits of common standards and address concerns in other ways, wherever possible, will reap rewards;

2) Work with the full range of existing multilateral institutions to incorporate and address the new issues raised by technology. Precedent and already-agreed rules provide a basis for extending agreements to the technology arena. Examples include a greater focus on digital trade liberalisation at the World Trade Organisation; new approaches to socio-economic development in lower income countries at the World Bank; and the extension of Interpol to tackling cybercrime. Nonetheless, progress can be slow in the large multilateral organisations, all the more so in the current geopolitical environment. In Asia, newer groupings such as CPTTP and RCEP in trade are well-placed to incorporate digital aspects from the start, while not being 'digital-only' agreements;

3) Recognise that more rapid progress on issues such as trade, technology and data flows can be achieved by working in parallel with smaller groups of 'like-minded' countries, such as G7, US-EU, G7 + 4, OECD, Five Eyes and the Quad. Determine the right mix (which topic in which grouping) through exploratory discussions and specific draft policy proposals. Such an approach should preserve flexibility in what the term 'like-minded' means. Be clear that such

groupings do not exclude other countries that are willing to sign up to the same terms of engagement. In a sense, 'like-minded' simply means an ability to agree to and comply with certain policy proposals.

4) Address issues of regulating Big Tech corporate behaviour primarily through US-European cooperation, recognising that, while both are major markets, it is the US that is headquarters to almost all the relevant companies. China has already embarked on the task of regulating its own Big Tech companies more stringently;

5) Explore how to expand regulation and oversight of Big Tech beyond US-Europe using the approach to global financial regulation and stability (Financial Stability Board, Basel Committee) as analogy. This would build on emerging national regulatory structures; provide a mechanism for including in the global dialogue other countries who are greatly affected by Big Tech (from the US and China) and indeed China itself; and, finally, expand the scope of oversight to any other questions of system stability that a putative 'Internet Stability Board' might identify;

6) Remember agreements between countries with divergent approaches can be even more valuable than those between like-minded countries. Accordingly, advance bilateral or minilateral discussions in the ambiguous but critical issue of cyberattacks, with the aim to agree 'rules of the game', 'red lines' and how compliance with these will be monitored. Where meaningful agreement proves out of reach, simply the direct communication of individual country positions on behaviour/ response can reduce uncertainty.

7) Address the additional uncertainty and risks from military applications of AI and other new technologies through primarily bilateral and minilateral discussions. Where agreement is not possible, continuing dialogue on even the most sensitive issues can at least identify and frame the issues and risks that each country is managing.

8) Maintain energy behind broader, more-inclusive initiatives (often UN-centred) that aim to build consensus on how to regulate technology (e.g. digital taxation), share its benefits (e.g. support to lower-income economies) and address security risks (e.g. bans or agreements on specific uses of technology – analogous to the chemical weapons ban). Such broader initiatives may also build momentum for direct smaller-group discussions between the major actors;

9) To enable these efforts, recruit, develop and train cohorts of policy professionals at national and international level who combine policy formulation experience with an up-to-date understanding of key technologies and business models.

Wise investments in global digital governance allow countries to address concerns on security, societal values and anti-competitive behaviours while limiting the impact on economic productivity, innovation and entrepreneurialism. They promise a better path to maintaining the benefits of common standards, cooperation on technological innovation and competitive, open trade – while ensuring that security and values are not compromised.

JESUS COLLEGE
CAMBRIDGE

Global Issues
Dialogue Centre

Global Issues Dialogue Centre
Jesus College
Cambridge
CB5 8BL
www.jesus.cam.ac.uk/research/global/Global-Issues-Dialogue