TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: A Model to Save Its Future

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Contents

Contents

An eight-part report that sets out international frameworks and a new model to save the global, open internet.

Key Points

The global, open internet is under threat. Restrictions on internet freedoms are increasing globally, governments are competing to assert their authority and a decades-long governance system of voluntary, technical bodies is now creaking. China is a growing competitor and adversary in many areas of internet governance yet remains an important partner in others, such as global infrastructure rollout.

Three tipping points make urgent action necessary: 1) Geopolitical competition is now playing out on hidden frontiers of conflict around the internet's architecture – including semiconductor supply chains, submarine data cables and technical standards – which may lock in fragmentation; 2) Globally, 3.7 billion people are yet to gain internet access, but as they do the world cannot rely on US hegemony to protect the future of the internet; 3) Restrictive internet models – which include censorship, internet shutdowns and political control of the internet's underlying architecture – are gaining ground, at a cost to the whole world.

Existing international alliances and institutions are falling short in protecting the future of the internet. Our report, presented as a series, sets out a new model of *internet internationalism* that reassesses states' core interests and identifies novel coalitions that combine security guarantees with commitments towards an open internet. We recommend that:

1. **D10 countries establish a Digital Infrastructure & Defence Alliance (DIDA).** This would be a novel coalition starting with, but not limited to, Australia, Canada, France, Germany, India, Italy, Japan, South Korea, the UK and US. These nations would cooperate on collective internet security and supply chains; regulatory coordination, including a mechanism to discourage internet shutdowns; cybersecurity; and global infrastructure to compete with China's Belt and Road Initiative. Importantly, the alliance should create trade, security and economic incentives to encourage other countries to join up.
2. **The UN creates a "Strategic Geopolitical Status" designation as part of a new geopolitical settlement with global tech**. Applicable to large technology firms with global geopolitical importance, this would require the creation of a self-regulatory, industry-wide body, with Permanent Observer status at the UN. Firms would also be required to set out an explicit "international policy" detailing their roles as proponents of an open internet.
3. **The UN, D10 and Strategic Geopolitical Status firms establish a Multi-Stakeholder Panel on**

Internet Policy (MPIP), modelled on the Intergovernmental Panel on Climate Change, to oversee the ecosystem. Composed of nation-states, civil-society organisations and industry, the MPIP would provide an early-warning system about the health of global information and communication networks. Additionally, it would evaluate progress on reforms, including institutional, where a lack of accountability has traditionally held them back.

4. **All countries, at minimum the D10, create foreign-policy strategies integrating digital, data and technology into diplomacy.** This would include empowering a new cadre of technology diplomats and ambassadors to align siloed approaches to internet and foreign policy, and to build state capacity to enable coordination across global-technology issues including cybersecurity, technical standards and platform regulation.

Foreword by Tony Blair

Harnessing the technological revolution in support of progress is one of the fundamental imperatives of the 21st century. Just as roads and railways connected towns and villages that once lived in isolation, the open internet now connects nations and communities. It allows for new forms of trade, new exchange of knowledge and ideas, and new channels to communicate and coordinate for the betterment of those willing to share.

But the technological revolution has been a global phenomenon unlike any other. Now, in response to the disruptive power of the open internet, new types of control are emerging. These can take many forms – from the responsible and necessary regulation of online platforms to make them safer and more accountable, to heavy political censorship or internet shutdowns that are increasingly used by authoritarian regimes. Put together, this leads to a great fragmentation in the global internet, and it is a fragmentation happening at the technical layer, the philosophical layer and the political layer.

The global trend over the past five years has been more restrictive internet models. Yet leaders should beware that such controls are illusory and short-sighted: as this report shows, there is no path to prosperity enabled by technology that also undermines core internet freedoms.

Faced with this new reality, the world's liberal democracies, instead of putting up a progressive, united front against the rising tide of internet authoritarianism, have retreated inwards, prioritising battles about their own internet sovereignty over long-term protection of the open internet.

The idea of recreating digital borders to replicate national ones has been picked up by governments across the world. At first it seems persuasive but on closer examination doesn't survive contact with technical or economic reality and is often an internet-era re-articulation of protectionism.

This report sets out a new model of "internet internationalism", which seeks to close the digital divide, bringing the 3.7 billion people without internet access online through global cooperation, and to build new alliances capable of preserving the economic and social benefits of the internet, while addressing the real need states have for solutions to online safety, cybersecurity and semiconductor supply chains.

It is also the time for the world's largest tech companies to step up and take responsibility. The global technology industry needs to be much better at conceptualising and being accountable for the impacts of what is akin to their own foreign policies, and actively uphold liberal values in international governance institutions.

The lesson of the Covid-19 pandemic is that the institutions of the 20th century are fundamentally mismatched to the challenges of the 21st century. To tackle increasingly complex crises such as climate change, pandemics and global poverty, we need new tools, new ideas and an interconnected global system capable of harnessing the technological revolution. Nationalism, fragmentation and protectionism will leave the world's citizens behind. Part of this must be a new mindset that looks to protect the entire internet ecosystem. Taking a truly internationalist approach will help tilt the future towards a more progressive, sustainable, universally accessible and globally beneficial internet.

Tony Blair
Executive Chairman

Understanding the Problem

Today, just over half the world's population – 51 per cent – is connected to the internet. It represents the world's most important economic and social infrastructure, enabling public services, businesses large and small, and global communities to operate at scale. But the principles of openness, permission-less innovation and resilience upon which the internet was founded are now faltering. Increasing restrictions on freedoms, regulatory and technical fragmentation, and a new era of geopolitical competition have left the open internet on the brink.

Political discussion about technology almost exclusively focuses on the issues that most visibly affect the public and the economy, such as content moderation, competition, tax and data privacy. These are serious and demand attention, but progressive leaders should also be concerned about the challenges that lie beneath the surface.

The stability of the global, open, interoperable internet has long depended on US hegemony, but this is increasingly giving way to a multipolar world where powerful states, emerging economies, industry, voluntary forums, multilateral bodies and crypto innovators each have a stake in the future. Both overt and covert tactics by these actors to gain control over the internet – often through small, imperceptible steps – threaten its future potential.

Global leaders need a new framework to navigate a world increasingly shaped by tensions over issues such as semiconductor supply chains, submarine cables and technical standards; the immense geopolitical power of today's largest technology companies; and the expansion of authoritarian internet models, driven predominantly by China but gaining ground across emerging economies.

While the internet has primarily been developed, maintained and governed by voluntary technical bodies for decades, in the face of these new challenges this model is creaking. In response, both liberal and authoritarian countries are stepping into the vacuum, seeking to assert influence. At one end of the spectrum, instead of putting up a united front to safeguard the open, global, interoperable internet, many liberal democracies have turned inwards, prioritising their own internal battles over internet sovereignty, as seen in plans for localised data infrastructures. At the other, China has adopted an overtly authoritarian model – facilitated by infrastructure investment, social-policy design and standards development – which it is encouraging low- and middle-income countries (LMICs) to adopt.

These challenges present stark, urgent risks: without an effective response, electronics shortages will continue, small businesses and high-growth start-ups won't be able to compete in international markets, and 3.7 billion people who do not yet have an internet connection may not gain access to the full benefits and freedoms of the global internet. In the long term, the cooperation necessary to tackle the climate crisis and future health crises such as pandemics will also suffer if solutions that rely on frictionless data-sharing and communication cannot come to the fore.

However, neither the perception of systemic complexity nor the challenge of international cooperation should deter countries, companies and voluntary bodies from seeking solutions. Recent G7 negotiations on a global tax deal and EU–US collaboration on trade and technology policies have shown that leaders have both the agency and opportunity to shape the underlying internet ecosystem. But acting urgently is all the more important because we are fast approaching three underlying tipping points:

1. Locked-In Fragmentation: The ideological divide between the regulatory models of the US, EU, China and others is often described as the “splinternet”. However, there are also hidden frontiers of conflict around the internet’s architecture, including semiconductor supply chains, submarine data cables and technical standards. In contrast to regulation, which can be aligned at any time, decisions about these underlying structures cannot be reversed in the future without significant upheaval and economic cost. This means fragmentation and friction may be locked into the internet’s architecture for good.

2. Emerging Internet Economies: Approximately 3.7 billion people still have no access to the internet. The LMICs that are home to most of this group will come to determine the future of the internet as connectivity increases and, on the current trajectory, it is likely they will receive the necessary financing from China. In the long run, progressive leaders can no longer rely on waning US hegemony to secure the internet’s long-term health. Instead, they must identify novel alliances to stabilise it through global interdependence.

3. Restrictive Models Are Costly and Gaining Ground: As states have increased their capacity to monitor populations, control the private lives of citizens, censor access and remove the benefits of a digital life entirely, the human rights costs have been significant. Authoritarian models have proved effective at shutting down dissent, and as a result of minimal international challenge they now are expanding. But such restrictions come with high domestic costs, stunting the trust in infrastructure required for e-commerce, foreign investment and innovation while reducing the potential of economic betterment for all. There are also immense costs to the global economy and the international community’s foreign-policy capability, which are often overlooked by the liberal countries who are affected.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Origins and Evolution

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- The economic and social value generated by the internet is based on core technical and governance principles: interoperability, permission-less innovation, security, resilience and physical infrastructure that is unaware about the content being communicated (known as "dumb pipes").
- Several countries, companies and multilateral governance institutions shape the development of the internet. The US has been historically dominant but in time this will shift.
- Led by China, more restrictive internet models are gaining ground on the open, liberal, Western internet model.

The internet is often referred to by a series of immaterial metaphors – "cloud", "web", "cyberspace" or even "information superhighway" – but little about how it really works is made visible. This grounding is important: understanding how the different physical and virtual layers of the internet combine is necessary to reveal who has control over the internet, where that power comes from and why it matters.

How Does the Internet Operate?

The internet is often illustrated as a vertical “stack” of physical and virtual layers. The Open Systems Interconnection (OSI) conceptual model breaks this down into seven layers while the TCP/IP model, which describes how these layers practically combine in today’s internet, contains four layers:

Figure 1 – Layers of the internet stack

OSI Conceptual Model		**Explanation**	**TCP/IP Model**
Application	*Application*	Provides user interface, e.g. Facebook or BBC News	**Application**
	Presentation	Formats data packets into application-ready text or audio/visual formats, and vice versa	
Logical	*Session*	Controls connections between devices and rest of network, creating and terminating connection sessions	
	Transport	Co-ordinates transfer of data packets between devices and the network, e.g. using protocols such as TCP	**Transport**
	Network	Defines how data is routed around a network, e.g. using IP addresses	**Internet**
Infrastructural	*Data Link*	Translates binary data (electrical pulses) into signals	**Network Access**
	Physical	Hardware layer, e.g. undersea data cables	

Source: Adapted from Article 19

Several features of the original vision behind the internet have contributed to its enormous social and economic importance today:

- The internet's architecture was built to commonly agreed standards that enable **interoperability** and communication between different devices and networks with minimal friction. This **interconnectedness** is the foundation upon which a single, global internet and economy is enabled.
- Open protocols mean that anyone can build tools and services based on these standards **without needing permission**. This paves the way for massive experimentation and innovation.
- Each layer of the internet stack was intended to be **independent** from others, limiting the ability for any single political or corporate actor to control the entire system. This ensures the rules that govern the internet cannot change without consensus, and this stability promotes investment and innovation.
- The global internet is, ultimately, a *network of networks*, each of which is designed to be relatively autonomous and **resilient**, and also ensuring that **power is distributed** throughout the network.
- At the bottom of the stack, data is transferred via physical and virtual networks that transport packets of information without being aware of their content. This model of **dumb pipes** limits preferential transporting and censorship.

While these conceptual layers of the internet mostly still hold today, the technologies and business models of internet companies have evolved significantly. This shift is often referred to as a transition between three eras:

Figure 2 – Internet paradigms

	Web 1.0	**Web 2.0**	**Web 3.0**
Period	1969–2004	2004–ongoing	2019–ongoing
Key characteristics	Open, permission-less protocols	Closed platforms and services	Decentralised applications (e.g. built on blockchain)

Economic value captured by innovators	No	Yes	Yes
Barriers to entry for new users	High	Low	High, but becoming much easier
Examples	TCP/IP, HTML, SMTP/IMAP	Facebook, Twitter, Google, Adobe	Ethereum, Bitcoin

Source: TBI

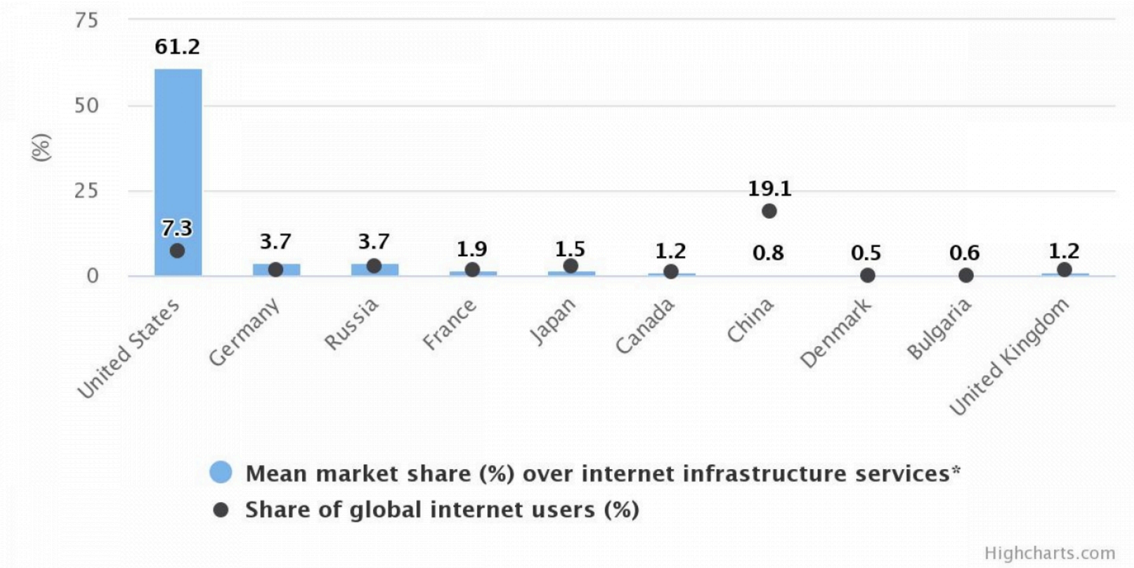
Who Controls the Internet?

The original vision of the internet was built on a patchwork of norms, policies and technical standards that were designed to avoid centralised control. While much of this architecture has remained distributed, some nation-states, technology companies and multilateral organisations have increased their roles in shaping the future of the internet. Smaller companies, emerging economies and the global internet community are often left out.

Countries

Europe, China and India are growing players in internet geopolitics but the US, in particular, has immense jurisdictional power by setting the regulatory environment for many of the internet's largest companies. Despite only 7.1 per cent of the world's internet users being based in the US, it is home to some of the most influential consumer tech companies and, on average, houses over 60 per cent of core infrastructure services for the global internet. This includes *data centres* – which store content for websites, databases and applications – and *DNS servers* – which tell your browser to convert URLs like en.wikipedia.org into an IP address like 208.80.154.224.

Figure 3 – Jurisdictional power over internet infrastructure versus share of global internet users



Source: Nick Merrill, The Internet Atlas Project, accessed 17 September 2021

*Note: *(DNS servers, web hosting, data centres, SSL certificates, top-level domains, server locations, proxy services) - May 2021*

Companies

As the web has developed – reducing costly friction and allowing innovators to capture some of the economic value they generate – many companies have also grown to extend significant influence over different aspects of the global internet. Many of these are large, well-known firms. For example, Apple and Google set privacy standards for a Covid-19 contact-tracing API; Facebook created a new "supreme court" to oversee its moderation decisions; and Twitter explored a new protocol to decentralise social media. All these decisions challenge nation-states' historical monopoly over global policy. These companies also wield significant economic power, such as when setting rules that govern how other companies can monetise services through app stores or by implementing proprietary technologies that become de facto standards for all.

Beyond user-facing services, however, are a set of infrastructure companies that are increasingly coming under scrutiny. In one recent example, a failure at Fastly – a content delivery network (CDN) that physically stores content closer to where users are based globally, to speed up load times – affected access in some geographies to popular websites including the *Guardian*, GOV.UK and Amazon. As sociologist Susan L Star wrote, this exemplifies how infrastructure often only "becomes visible upon breakdown". While it may be tempting to bemoan the single points of failure that lead to these breakdowns, the reality is that the costs of building in the redundancy required to avoid these issues, by contracting with multiple companies simultaneously, are often more than a short period of downtime.

Beyond accidental failures, some infrastructure companies also have taken deliberate actions that illustrate their power. For example Cloudflare, another CDN, has denied service to websites 8Chan and The Daily Stormer – which had repeatedly failed to remove or moderate far-right, abusive, violent content – making it difficult for those sites to operate. While these decisions broke with a general precedent that content moderation should primarily happen at the application layer by user-facing services, these user-facing websites had failed to moderate so Cloudflare took action at the infrastructure layer.

Content neutrality remains an important default principle for services further down the stack. However, with other infrastructure services including payments, web hosting and search companies under pressure to act on abusive content, these firms are increasingly left to evaluate their responsibilities with little legal guidance or regulatory support. For example, Cloudflare has recently launched extra cybersecurity support for at-risk public interest groups and state elections. While the power of infrastructure companies is clear, it is a lack of due process and internet infrastructure policy frameworks that is the primary issue.

Decentralised Web 3.0 Organisations

The transition from Web 2.0 platforms to Web 3.0 protocols will also challenge incumbent gatekeepers. For example, while traditional currencies require a single authority, such as a bank or government, to maintain a record of transactions and prevent double spending, transactions of decentralised digital currencies like Bitcoin are verified computationally by consensus mechanisms such as proof of work or proof of stake, with no need for central authorities. Ethereum, another decentralised currency, is also a protocol incorporating programmable contracts whereby payments are automatically made on the basis of some condition being fulfilled. At scale, this could enable entire organisations to be managed autonomously in code, rather than by individuals in a bricks-and-mortar office.

While nation-states retain some levers to control Web 3.0 applications – for example, so-called on-ramps, such as cryptocurrency exchange platform Coinbase, are regulated financial entities – they have limited ability to regulate the underlying protocols except by participating directly in their development, which in turn could devalue any individual protocol's appeal to the wider crypto community. While we are only at the beginning of the Web 3.0 era, as it matures it promises to disrupt what is already an unstable power dynamic between states, technology companies and the global internet community.

Global Institutions

Finally, there is a group of multilateral, multi-stakeholder, international governance bodies that collectively maintain and develop the global internet. While these organisations have been fundamental in the formation of the internet, they have also struggled to keep pace with its evolution and now their role is being challenged.

Figure 4 – Internet governance institutions

Acronym	*Full Name*	*Focus*	*Origin*	*Type*
IGF	*Internet Governance Forum*	Internet policy	**2005**. IGF set up as forum for discussion re: internet policy and governance	UN multi-stakeholder forum and regional dialogues

ITU	*International Telecommunications Union*	Internet infrastructure and technical standards (incl. radio, satellites, other ICTs)	**1865**. Set up to connect international telegraph networks. Became UN agency in 1949	UN agency
W3C	*World Wide Web (W3) Consortium*	Develops web standards	**1994**. Founded by Tim Berners-Lee to develop web protocols and guidelines	Voluntary standards body, funded by members
IETF	*Internet Engineering Task Force*	Develops and promotes internet standards, incl. TCP/IP	**1986**. Originally supported by US federal govt, but since 1993 funded by *Internet Society*	Voluntary standards body
ISOC	*Internet Society*	Advocacy re: internet standards, access, skills and policy, incl. funding for **IETF**	**1992**. Set up by Vint Cerf and Bob Kahn. In 2002, ICANN gave ISOC Public Interest Registry (PIR) to generate revenue from .ORG domains	Non-profit / charity. Funded by .ORG profits. Sale of PIR to private equity in 2019, to create an endowment, was aborted

ICANN	*Internet Corporation for Assigned Names and Numbers*	Manages IP addresses and DNS / domain names	**1998.** Technical maintenance for IP address and DNS root	Non-profit / charity
UNICODE	*Unicode Consortium*	Maintains and develops the Unicode Standard, which ensures text can be shared between languages and borders without corruption, including approving new emoji	**1991.** Established to create and maintain a standard for multilingual text representation	Non-profit, funded by membership fees and donations. Voting members include Adobe; Apple; Facebook; Google; Microsoft; Netflix; SAP; Salesforce; University of California, Berkeley; Bangladesh Computer Council; Emojipedia; Tamil Virtual Academy; and Yat Labs
GIFCT	*Global Internet Forum to Counter Terrorism*	Information sharing for countering online terrorism	**2017.** Founded by Facebook, Microsoft, Twitter and YouTube	Tech-industry funded initiative
IWF & NCMEC	*Internet Watch Foundation (UK)*	Child safety and protection; hashing	**1996 (IWF).** ISPs + London Internet Exchange initiative to	Non-profit / charity

	National Center for Missing & Exploited Children (US)	databases for spotting CESA content. IWF and NCMEC entered data-sharing agreement in 2019	provide URL database to enable CESA content blocking. Now includes a broad membership of tech companies and education providers **1981 (NCMEC).** Missing children's charity funded by US Department of Justice	
Five Eyes	*Five Eyes*	Intelligence sharing	**1940s.** Set up to counter Russia's growing sphere of influence pre- and during Cold War	UK, US, Australia, Canada, New Zealand alliance
DN	*Digital Nations*	Digital government collaborative network	**2014.** Initially D5: UK, Estonia, Israel, NZ, Korea	Diplomatic network

Source: TBI

Openness Versus Authoritarianism

The foundations of today's internet are based on openness, permission-less innovation, security, stability and global interoperability. These features, and the limited friction and intervention they entail, have enabled the internet to grow and act as one of the world's most important economic and social infrastructures.

However, as the internet has grown in importance, regulations have followed. Some restrictions are clearly necessary – a libertarian "state of nature" would do little to ensure privacy or safety while the meme of an unregulated "wild west" is misleading. But nation-states are looking to reimpose their authority. Even governments in free societies are considering increasingly interventionist steps on internet architecture – be it bans on encryption or anonymity, data localisation laws, censorship or full internet shutdowns. At the most extreme end, China's internet model is the archetypal authoritarian approach, given its extensive domestic and international censorship as well as requirements on foreign companies to create local subsidiaries and store data in the country to enable surveillance.

However, many other jurisdictions, including the EU, are also considering data-localisation laws as part of a growing global trend towards policies that promote the idea of digital sovereignty. It is not unreasonable to require data to be stored in a jurisdiction where countries have a stake in its governance. Yet for some smaller countries in particular, this comes with trade-offs. Putting up new digital borders could impede access to the global internet economy, while data-localisation laws could also cut countries off from hyperscale data centres and technical services – and their immense economic and technical benefits – if they are located outside their borders.

Leaders must beware a death by a thousand cuts: the stability, openness and interoperability of the global internet are a public good – generating prosperity and opportunity for the long-term – and they are increasingly at risk.

Charts created with Highcharts unless otherwise credited.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Hidden Frontiers

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- The internet is splintering along ideological lines, with many governments – in particular the US, China, EU, India and Russia – competing to reassert the authority of nation-states.
- Fragmentation is now moving down to the internet's fundamental, hidden infrastructures: technical standards, supply chains and submarine data cables.
- In contrast to regulatory divergence, which can be addressed in the future, these structural battles risk locking in friction and fragility at great cost. The greater the intervention lower down the internet stack, the higher the risk that fragmentation may be locked into the internet's architecture for good.

One benefit of the global, interoperable internet is that it avoids much of the traditional friction that comes from physical borders. Communication and transactions are near-instant, breaking many geographical constraints. But as states try to reimpose their authority by regulating both the good and bad of the internet's disruptive potential, this global infrastructure may splinter into many sovereign internets. This phenomenon risks undermining the principles on which decades of economic and social opportunity have been based.

Shedding Light on the Splinternet

While the regulatory component of this so-called splinternet has been covered at length elsewhere, states are increasingly intervening deeper down the internet stack to assert control on the fabric of the internet itself. The battles at this hidden frontier are part of a new and more worrying trend. While regulatory divergence creates challenges of its own, regulations are malleable and can be revisited and aligned in future. In contrast, structural changes to the standards, supply chains and submarine cables that underpin the internet cannot be reversed without significant upheaval and economic cost. The greater the intervention lower down the internet stack, the higher the risk that fragmentation may be locked into the internet's architecture for good.

Revisiting the Four Internets Model

Internet fragmentation has been the subject of many academic analyses. In 2018, Hall and O'Hara set out the battle between four competing ideological models:

1. The technology-centred *Silicon Valley model* that focuses on maintaining an open internet to reflect its original, idealistic vision.
2. The rights-based *European model* that seeks to minimise uncivil behaviour such as harmful content, anti-competitive practices and privacy intrusions, even if it could come at the cost of innovation.
3. The surveillance-driven *authoritarian model*, led by China but becoming increasingly attractive to other nations seeking greater controls through enhanced surveillance and identification powers in the name of "social cohesion".
4. The *DC Commercial Internet model* favoured by former President Donald Trump that advocates for the interests of private actors over the public good of an interoperable system.

However, as rapidly as the internet ecosystem proliferates, these four visions have given way to multiple models of a sovereign internet – each driven by differing priorities but united in their aspiration for control:

Figure 5 – The internet risks fragmenting due to an ideological battle of sovereign internets

Jurisdiction	Regulatory model	Key feature	Challenge
US	Laissez-faire/lack of friction	Low barriers to entry help innovation	Superstar companies dominate
Europe	Strong public-values regulation	De facto global regulator	Bureaucracy stifles innovation, creating few major players and limiting geopolitical leverage

China	Authoritarian control	Huge market mitigates regulatory constraints	State champions dominate; civic restrictions
India	Tight control of infrastructure; limited but growing regulations for services	Huge market creates geopolitical counterweight	State champions dominate; civic restrictions
Russia	Authoritarian control	Successful tests of a “national internet” enable censorship at scale	Weak internet economies; civic restrictions

Source: TBI

Standards, Semiconductors and Submarine Cables

These national internet models provide a snapshot of the overt regulatory approaches to influencing the development of the internet, but underneath them lies a web of technical standards and hardware that is becoming a new, hidden frontier of geopolitical competition. When examined individually, the motives of states could be viewed as benign or even beneficial. However, when aggregated, the potential effect of these attempts to assert control over fundamental structures of the internet may lock in global fragmentation for good.

Fragmentation Through Competing Standards Proposals

As set out earlier, the layers of the internet stack are largely independent and unaware of each other. A new proposal from China called New IP, in practice submitted by Huawei and other industry collaborators, would involve a shift away from this model. It seeks to reconceptualise the network layer of the internet (the dumb pipes), which ordinarily transports data packets without being aware of content. There are two main consequences of this:

1. **Political control of the network**: Data packets contain both content and descriptions of where they are being transmitted. By enabling surveillance techniques such as deep-packet inspection, New IP could break the independence of this network layer – so the dumb pipes are no longer dumb – and enable political interference.
2. **Traceability:** Descriptions of New IP contain references to indelible identifiers and blockchain architectures that cannot be edited and would enable complete traceability of content and networks. This contrasts with today's system of temporary IP addresses, which provide devices with some level of identity protection. In essence, as internet governance expert Carolina Caeiro argued at the 2021 RightsCon Summit, this proposal would turn the network into a surveillance tool.

The proposals are sold on the idea that the internet's current architecture cannot support today's accelerating growth in traffic, so a new model is needed. The moves towards greater digital sovereignty are also a response to the dominance of foreign infrastructure providers such as NEC, Fujitsu, Ericsson, Siemens, Alcatel and others in China's telecoms markets in the 1980s and 1990s. There are many more secure, privacy-protecting and technically neutral solutions to the New IP model and its lack of any clear provisions to protect privacy and other rights. There is also growing concern that New IP could lead to the type of capture, transfer and use of personal data that violates states' obligations under international human-rights law.

Figure 6 – Comparison of current internet standards and governance model versus China's New IP proposal

Telecoms & technology stack (OSI model)		Technical model		Governance model	
		TCP/IP model (Current)	China's New IP proposal	Current model	China proposal
7	Application	Application	Third-Party Application	Industry, W3C	W3C, ITU
6	Presentation			IETF, W3C	
5	Session		Resource Management	IETF, W3C	ITU
4	Transport	Transport		IETF, W3C	
3	Network	Internet	Blockchain	IETF, ETSI	
2	Data Link	Network Access		3GPP, IEEE, ETSI, ITU	
1	Physical		Physical	3GPP, ITU, ETSI, GSMA	3GPP, ITU

Source: Stacie Hoffmann, Dominique Lazanski & Emily Taylor, "Standardising the splinternet: how China's technical standards could fragment the internet" (2020)

The New IP proposal also threatens the future of multi-stakeholder governance institutions that traditionally oversee the design, development and maintenance of internet standards and protocols. Instead, China proposes that the International Telecommunication Union (ITU), a UN body in which only nation-states can vote, should be empowered at the expense of bodies like the Internet Engineering Task Force (IETF). This means bypassing the multi-stakeholder standards organisations that incorporate voices from industry, civil society and governments, and which largely support a free and open internet. In turn, China's proposal provides the opportunity for national governments, which support more tightly censored and regulated models of the internet, to have greater power in shaping its future.

Currently, China's New IP proposals have been rejected by the IETF and other multi-stakeholder bodies but have gained some traction at the ITU. The proposals may return in different forms if they are not immediately successful. However, while international standards can facilitate adoption of technologies, they are not completely necessary. China is already piloting New IP domestically and may look to export it to emerging digital economies that are dependent upon Chinese investment and infrastructure in the absence of effective alternatives.

Fragmentation Through Semiconductor Supply-Chain Competition

Semiconductors have become a critical, foundational technology and strategic industry in the 21st century. Supply chains are highly globalised: chip architectures are routinely designed in the US or UK but fabricated in Taiwan or South Korea. However, a recent US White House supply-chain review expressed the need for more self-reliance in chip production. This is catalysed by national security concerns, given China's ongoing territorial claims over Taiwan, which could threaten the world's leading chip manufacturer, TSMC.

The frontier for commercial production, at present, is developing process nodes at 3 nanometres (nm). While US firm Intel has plans to offer this capability, only TSMC and Samsung (South Korea) are in advanced stages of doing so. Beyond the US, South Korea and Taiwan, no other country, including China, boasts a semiconductor manufacturer that is near this milestone.

Figure 7 – Global semiconductor manufacturing capability

Major Industry Players		Process node (nm)								
Country	**Company**	**90** *(2003)*	**65** *(2005-07)*	**45/ 40** *(2007-09)*	**32/ 28** *(2009-11)*	**22/ 20** *(2012-14)*	**16/ 14** *(2015)*	**10/ 7** *(2016-19)*	**5** *(2020+)*	**3** *(~2022)*
Taiwan	TSMC	▣	▣	▣	▣	▣	▣	▣	▣	⚙
South Korea	Samsung	▣	▣	▣	▣	▣	▣	▣	▣	⚙
USA	Intel	▣	▣	▣	▣	▣	▣	⚙🌐	⚙🌐	⚙
UAE	Global Foundries	▣	▣	▣	▣	▣	▣	▣		
China	SMIC	▣	▣	▣	▣	▣	▣	⚙		
South Korea	SK Hynix	▣	▣	▣	▣	▣	▣	▣		
Japan	Kioxia	▣	▣	▣	▣	▣	▣			
Taiwan	UMC	▣	▣	▣	▣	▣				
Switzerland	STM	▣	▣	▣	▣	▣				

Germany	Infineon	▣	▣	▣	▣
USA	IBM	▣	▣	▣	▣
USA	Texas Instruments	▣	▣	▣	▣
Japan	Fujitsu	▣	▣	▣	

Example products using chips built at each process node

90nm - Playstation 2
65nm - Microsoft Xbox 360
45/40nm - Playstation 3
32/28nm - Intel Core i3 and i5 processors
22/20nm - iPhone 6 (A8 chip, 20 nm)
16/14nm - iPhone 6S, iPad Pro (A9 chip, 14nm; A9X & A10 chips, 16 nm)
10/7nm - 2nd-gen iPad Pro (A10X chip 10nm), iPhone XS (A12 chip, 7nm), iPhone 11 (A13 Bionic chip)
5nm - iPhone 12 (A14 chip); M1 Macbooks

Key:

▣ Currently produced in commercial volumes

⚙ Under development/planned

🌐 Intel is in commercial production at 10nm. It has also made conceptual progress towards 7nm and 5nm but due to technical challenges it has recently outsourced 5nm production to TSMC

Sources: Eurasia Group and TBI

China's SMIC is lagging – it is currently only planning 7nm chips, which TSMC and Samsung are already producing at scale – while the US has also pressured TSMC not to sell to Huawei, one of China's largest technology vendors. As a result, as global demand for semiconductors has increased, the fixed supply of expensive chip foundries combined with US sanctions has created a shortage. One by-product of this is a new industrial hierarchy, with US tech giants the winners and carmakers, many of which are based in the

EU, the losers. Similarly, ASML, which supplies chip-manufacturing machines to the semiconductor industry and is the EU's biggest tech company by market capitalisation, has also been affected by US export controls on China.

While building new chip foundries in the EU and US may be rational given today's fractious geopolitical environment, the trade-off is likely added cost and complexity for global supply chains. As states increase their self-reliance when it comes to chip fabrication, there is a risk that device manufacturers may be forced to use specific manufacturers or foundries. While this is already happening to an extent given TSMC's dominance of the sector, partnerships based on political allegiances are worse for consumers because they reduce competition and create a greater risk of lock-in than those based purely on technical capability.

Fragmentation Through Proprietary Submarine Cables

Underpinning the global internet is a network of surprisingly vulnerable undersea cables. This backbone accommodates approximately 97 per cent of internet and voice data and facilitates around $10 trillion of financial transactions daily. There are four main suppliers: Alcatel Submarine Networks (France), SubCom (US), NEC (Japan) and Huawei Marine Networks (China). Increasingly, new players such as Google, Facebook and Microsoft are also investing directly in cable infrastructure to accommodate the massive web traffic they generate.

While submarine cables are not free of regulation, since the internet's inception there has been a consensus that the global free flow of data is a common good and, if regional variation is necessary or desirable, this should happen much further up the stack (for example at the content-regulation level). However, US pressure on Europe over China's "Peace Cable", a new cable travelling over land from China to Pakistan and then under the sea to reach France, cuts against this consensus. Huawei, which now controls almost 10 per cent of the subterranean market, is the third largest shareholder in the company building the new cable.

There are a number of physical and digital risks to submarine cables, and while most incidents are related to accidental activity there is legitimate concern of potential deliberate sabotage. Fears of surveillance and data theft through the creation of backdoors during cable construction, tapping landing stations or tapping cables at sea, as well of cyberattacks, are also beginning to dominate the policies and politics of subterranean cables. As geopolitical debates increasingly co-opt this foundational infrastructure, a variety of responses are possible: states may keep some traffic away from vulnerable cables, or trends towards digital sovereignty may expand to this layer, creating a race for proprietary submarine cables.

A network of sovereign cables could lead to huge inefficiencies in the global internet network, which relies on transporting information as fast as possible. It could also ultimately leave states more vulnerable if forced to rely on a smaller number of cables, instead of an interconnected global network with built-in redundancies. This is not an immediate risk, but leaders must be aware that subterranean geopolitical competition could splinter the internet at the very deepest level.

Charts created with Highcharts unless otherwise credited.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Economic and Social Costs of Restrictions

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- Fragmentation and restrictions on the global, open internet create immense social and economic costs.
- There is no path to prosperity enabled by technology that also undermines the core internet freedoms from which the leading digital economies benefit. Emerging economies should beware of taking regressive steps that could impede the growth of tech sectors.
- Internet shutdowns in particular have become a go-to lever for many leaders looking either to limit social disruption or explicitly repress populations. These steps curtail internet economies in the long term and have cost the global economy more than $13 billion since 2019.

As the internet has disrupted the global economy, many governments are increasingly responding via national regulatory responses. While this country-level approach may be in their narrow, short-term interests, they risk fragmenting the internet into national and ideological segments. This fragmentation could exacerbate the domestic issues that national regulation seeks to address, interfere with international intelligence and response mechanisms, and undermine international commerce and communication enabled by a fundamentally open, borderless internet.

Figure 8 – The risks of fragmentation

Category	**Fragmentation Risk**
Security	Technical variation introduces greater uncertainty into cybersecurity, increasing threat landscape
Innovation and Market Access	Requirements to federate across jurisdictions would create costly barriers for companies and start-ups wanting to operate globally

Human Rights	Citizens disenfranchised from global communication, information and trade
Governance	Processes, norms and institutions created to enforce responsible state behaviour are disrupted
International Order	Internet shutdowns – which reduce international visibility and delay response – are made easier
Future Cooperation	Reduced options to promote alliances or address future crises, e.g. cyberthreat detection or global health data sharing

Source: TBI

How Restrictions Create Costs

The cost of fragmentation to innovation is especially high. Companies facing divergent compliance duties face significant market entry and exit barriers, while the option of federating across different jurisdictions involves costs that favour the largest incumbents in those markets.

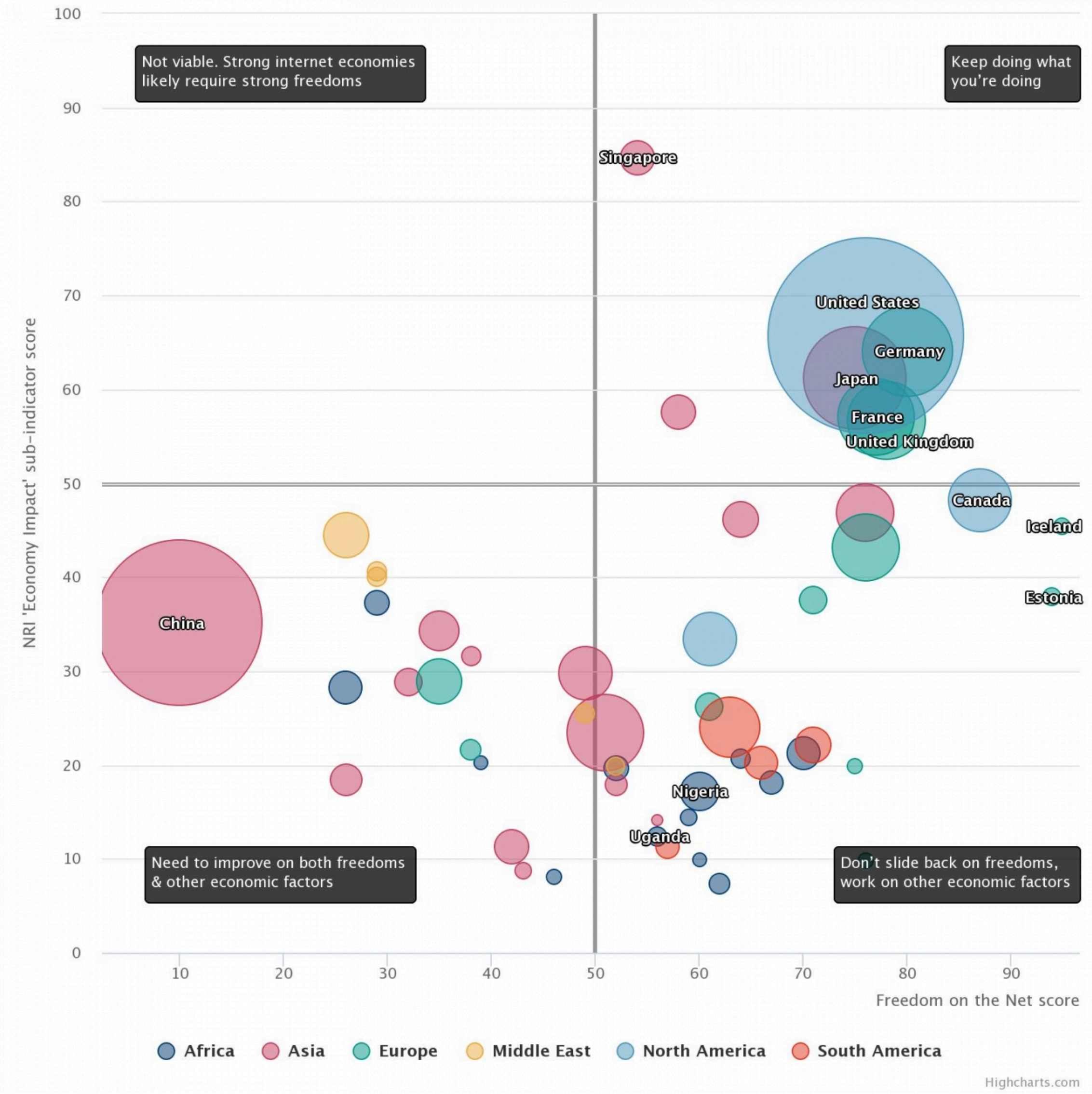
To operate globally, companies may need to structure themselves akin to Amazon’s regional companies. However, while trade tariffs and the logistical challenges of fast-moving consumer goods result in unavoidable frictions that may warrant local subsidiaries, divergence in internet regulations may create avoidable barriers to start-ups seeking to innovate globally. This further concentrates digital power and reduces economic opportunity for everyone else.

Economic Benefits of Internet Freedoms

Demonstrating the economic dividend of internet openness is challenging. Openness is necessarily subjective and hard to isolate quantitatively. China provides a counter-example of a fast-growing emerging economy with extensive internet restrictions – though its large domestic market means it may be an exceptional case. Furthermore, projecting the future potential of internet openness, in contrast to a more restrictive model that might otherwise preclude some economic gains, is difficult.

Mapping Freedom House's Freedom on the Net index against the Network Readiness Index's Economy Impact score – which indicates the financial impact of a country's participation in the network economy – can provide an initial illustration to complement qualitative case studies. While not a perfect measure, this analysis at least provides a snapshot of the economic dividend from internet openness at a macro level. The countries that maximise the internet's economic benefits are generally those with the strongest internet freedoms. Notably, the top-left quadrant is empty, indicating that internet freedoms may be a necessary, albeit not comprehensive, condition of a successful internet economy. [1] [2]

Figure 9 – 2020 Network Readiness Index economic impact score versus Freedom on the Net score for 2020



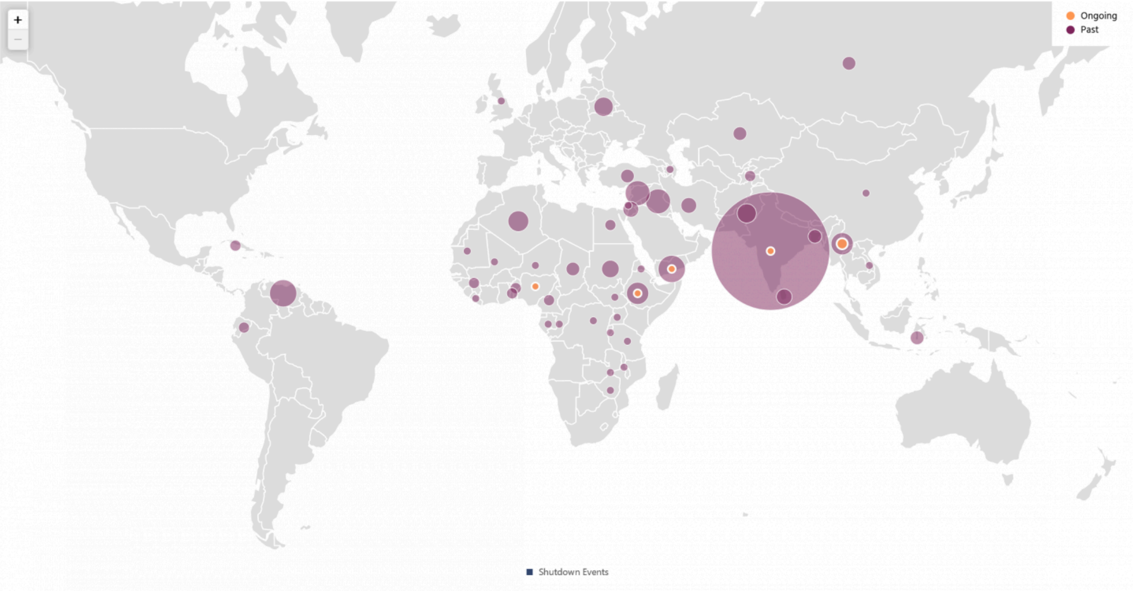
Sources: TBI analysis, Network Readiness Index, Freedom House

Even in China, where a large domestic market has allowed its internet economy to grow significantly despite restrictions, recent crackdowns on major tech companies such as Alibaba and Didi may have serious future implications for investor confidence in the Chinese tech ecosystem. Indeed, since March, there has been an extraordinary pattern of resignations among founders of some of China's largest companies, including JD.com, Bytedance (TikTok's parent company) and Pinduoduo. Similarly, a sell-off of Chinese tech stocks between February and July 2021 including Tencent, Alibaba, Meituan, Pinduoduo, Kuaishou Technology, JD.com, Baidu and Xiaomi resulted in over $800 billion in lost value. Further upstream, lower investor confidence may also have contributed to the apparent drop-off in unicorn start-ups in China.

Internet Shutdowns and Their Costs

Given this analysis, it is unfortunate that internet shutdowns, which exemplify some of the most extreme restrictions available, have become a costly, go-to lever for many developing countries to assert control.

Figure 10 – Internet shutdowns by country as of September 2021



Source: Internet Society Pulse. Data correct as of 14 September, 2021. Full sources and shutdown details available at: https://pulse.internetsociety.org/shutdowns

While typically associated with the total blackout of the internet, the term internet shutdown encompasses a much wider breadth of service disruptions with tremendous social and economic impact. Internet shutdowns include generalised network disruptions (full shutdowns), denial of access to specific websites (for example, social media), and throttling (slowing down internet connections to limit video sharing and/or disrupt communications, for instance).

Recent data on social-media censorship illuminates a worrying global trend on internet shutdowns. Of 180 countries analysed since 2015, 66 have blocked or heavily restricted social media during this period. Many of these are in Africa: 31 of 54 African countries (57%) have blocked access to social media to some degree since 2015.

Governments cite various reasons for shutting down the internet. According to an analysis by Access Now, the most commonly cited cause for shutdowns in 2020 was political instability, and their use most often justified as a “precautionary measure” in response to the risk of community violence. However, other rationales exist. Algeria and Iraq have cited exam cheating, and Nigeria and India have argued for shutdowns on the basis of access to hate speech and fake news.

While some shutdowns are overtly repressive, as with politically motivated interventions in Iran and Myanmar, others are in response to “information incidents” such as elections or natural disasters, which can shape the information environment in ways that, as Full Fact states, “make it harder to tackle misinformation effectively”. In these circumstances, some leaders, without defined levers for content moderation, have turned to shutdowns or service denials, fearing community violence. This is often linked to social-media services lacking moderation capability in local languages, which means content encouraging ongoing community violence may go unchecked.

Technology companies do need to invest more in local expertise, but it is not clear that shutdowns are an effective tactic for achieving leaders’ stated aims. Research on shutdowns in India, published in 2019 by the Stanford Global Digital Policy Incubator, suggests that internet blackouts can encourage violence by “compelling participants in collective action … to substitute non-violent tactics for violent ones that are less reliant on effective communication and coordination”.

Domestic Shutdowns Have Global Consequences

Turning to shutdowns as a policy lever restricts the growth of internet economies in the long term while also disenfranchising communities from global networks of communication and trade in the short term. This creates global costs that are routinely underappreciated. According to research by Top10VPN, since 2019, 235 major internet shutdowns in 44 countries have cost the global economy $15.5 billion.

There are foreign policy implications too. As Iran's shutdown in November 2019 first demonstrated, these measures not only disrupt domestic communications but help censor repression internationally – delaying any potential foreign policy response. Shutdowns are therefore not just a domestic issue: they impose significant costs on the global economy and reduce the international community's visibility and diplomatic capability.

As such, the focus should be on an international framework that provides a baseline against which to judge disproportionate responses. Even in the face of misinformation or harmful content, denying communities access to internet services comes at an immense cost to economic and social freedoms. While countries with small internet economies may see shutdowns as a small price to pay today, there are enormous costs in the long term as a result of unrealised gains.

Charts created with Highcharts unless otherwise credited.

Footnotes

1. ^ The methodology for Freedom House's Freedom on the Net report can be found here. The 2020 NRI Economy Impact is one of several sub-indicators that make up the Network Readiness Index. It is itself based on 5 further sub-indices: i) Proportion of medium- and high-tech industry value added in total value added (%), 2016; ii) High-technology manufactured exports (% of total exports of manufactured goods), 2019; iii) Number of applications filed under the Patent Cooperation Treaty (PCT) (per million population), 2017; iv) Labour productivity per person employed (2019 US$), 2019; and v) Average answer to the question: In your country, to what extent is the online gig economy prevalent? [1 = Not at all; 7 = To a great extent], 2018–19. Full sources and definitions can be found in Appendix II of the Network Readiness Index 2020 report, on p298.
2. ^ While this measure is slightly noisy – both indices are composite measures based on several sub-indicators – it is notable that the top-left quadrant is entirely empty: no country with a Freedom on the Net score of less than 50 achieved a score over 50 for NRI Economic Impact. While a strong Freedom on the Net score does not guarantee a strong NRI Economic Impact score (which covers broader 'participation in the network economy', and is thus determined by several other economic factors that may not be present in places with otherwise strong internet freedoms), this analysis suggests that internet freedoms may be necessary, even if not sufficient, for successful internet economies.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Geopolitical Cooperation Is Falling Short

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- Liberal democracies have failed to cooperate on protecting the future of the internet from authoritarian challengers.
- Despite shared values, cooperation is not as simple as commonly assumed. The EU and US, in particular, have competing policy objectives across a range of global technology policy issues.
- While China is often framed as a common threat for liberal democracies, it is not a monolith: it is a partner, competitor and adversary all at once. This requires a strategy that distinguishes between issues of collaboration, competition and confrontation rather than reverting to inaccurate cold-war narratives.

Instead of putting up a united front against the rising tide of internet authoritarianism, the world's liberal democracies have retreated inwards, prioritising battles about their own internet sovereignty over long-term protection of the open internet. Not only does this give free rein to authoritarians, it also undermines the credibility of liberal countries when they criticise other states for more restrictive internet policies, be it data-localisation requirements at one end of the spectrum, or full internet shutdowns at the other.

Why is cooperation and long-term thinking failing? First, although the US and EU are often natural allies, their objectives across a range of tech policy issues have historically been further apart than is commonly assumed. Second, the institutions designed to shape the future of the internet – both domestic government departments and international bodies – are ill-equipped to deal with an increasingly complex governance environment.

Clashing Objectives

As internet companies grow, serving millions of users around the world, the need for global alignment on regulatory standards has increased. To that end, the liberal democracies of the US and EU have long seemed like they should be natural partners on technology policy. Until recently, though, transatlantic debates about global standards on tax, data privacy, competition and content moderation saw few signs of progress. This is because, across many long-term issues, they have had fundamentally different geopolitical incentives and regulatory philosophies.

The US is home to several major tech champions. Many of these are vertically integrated multinationals that are systemically important to the global internet economy. Google, for example, provides both user-focused applications and core infrastructure services. In contrast, while there are some large tech companies based in the EU, they do not have the same sort of geopolitical leverage from which the US benefits. This is a fundamental source of tension, creating battles over so-called digital sovereignty, data localisation and privacy.

For example, since the EU's Court of Justice struck down the EU–US Privacy Shield (a transatlantic data-transfer framework), negotiations have stalled on a new deal to limit US intelligence agencies' access to EU data. In turn, the EU has been exploring data-localisation requirements and a European cloud infrastructure, which is out of step with more liberal data storage and transfer approaches in the US, UK, Australia and Japan.

Many in the EU also still see competition investigations against US tech companies as a crucial lever to reclaim some influence on the world stage of global tech policy. This has had pushback in the US, with the Digital Trade Caucus encouraging President Biden to resist this "targeting of American companies".

These tensions reflect broader philosophical differences. While the US is generally most concerned with *avoiding* bans on pro-competitive behaviour, the EU is focused on *regulating* anti-competitive practices. Similarly, Eric Schmidt, chair of the US National Security Commission on Artificial Intelligence and former CEO of Google, recently criticised current EU proposals on AI transparency as prioritising regulation over innovation, illustrating the competing priorities on each side of the Atlantic.

The result: US–EU cooperation is much less assured than is frequently assumed. However, US attitudes towards tech regulation have shifted with the change in administration. There are now discussions around a global tax deal and a new federal privacy law while the Federal Trade Commission (FTC), under new chair Lina Khan, has launched several antitrust lawsuits against large technology companies. Whatever the merits of these individual steps, they have had the effect of bringing the positions of the US and EU closer together and improving prospects for cooperation.

Figure 11 – The policy objectives challenging the assumption that cooperation between the US and Europe is certain

	Cooperation prospects (pre-Biden)	Cooperation prospects (post-Biden)	EU objective (current)	US objective (current)	Comments
Tax	✕	✓	Raise more revenue; achieve fair agreement	Protect US tech sector while raising revenue for new infrastructure	US incentives have changed with plans to raise domestic corporation tax, making a global tax deal possible. US remains opposed to unilateral digital taxes
Data Privacy	✕	•••	Export privacy standards; reclaim sovereignty	Limit the compliance duty barriers to innovation; retain sovereignty	US–EU Privacy Shield negotiations stalling, though California's CCPA is aligned with EU's GDPR and new Data Protection Agency mooted in US

Competition	…	…	Regulate against anti-competitive practices, including focus on *ex-ante*	Tackle size and power of big tech (bipartisan consensus now that these firms are too big)	US–EU Trade and Technology Council includes antitrust talks, with new FTC commissioner closer to EU position on competition. Contrast from previous US admin's tacit protection of domestic tech sector
Content Moderation / Intermediary Liability	✗	…	Digital Services Act will impose greater responsibilities on Very Large Online Platforms (VLOPs)	Liability protections, such as Section 230 of the US Communications Decency Act, have become politicised	Prospects for cooperation unclear
Cybersecurity	✓	✓	Protect itself and supply chain	Protect itself and supply chain	US and EU share common adversaries (state and non-state)

Key:

✗ Cooperation very unlikely

… Cooperation possible

✓ Cooperation highly likely/already existing

Source: TBI

China Is Not a Monolith

Tensions between China and the West are often described as a new cold war. This narrative is understandable, but misplaced. As this report has described, China's expanding authoritarianism does pose a great challenge to the future of the internet and liberal world order. However, so far, this has not been a sufficient threat for the US and EU to put aside any other differences and focus solely on resisting China. This is illustrated by recent EU–US disagreements over the ratification of the EU–China Comprehensive Agreement on Investment (CAI). While this is now faltering, and Italy has committed to review its Belt and Road Initiative deal with China, the EU remains wary of getting into a full trade war.

The truth is that binary narratives simply framing China as a common enemy are insufficient to encourage widespread agreement. China is not a monolith: it is a partner, competitor and adversary all at once. As we set out last year, responding to this reality requires a three-part strategic framework based on cooperation, competition and confrontation.

Applying this strategic framework to issues in internet geopolitics can help to cut through a debate that is often overly simplistic:

Figure 12 – The 3Cs: a framework showing how the West can manage China's growing influence

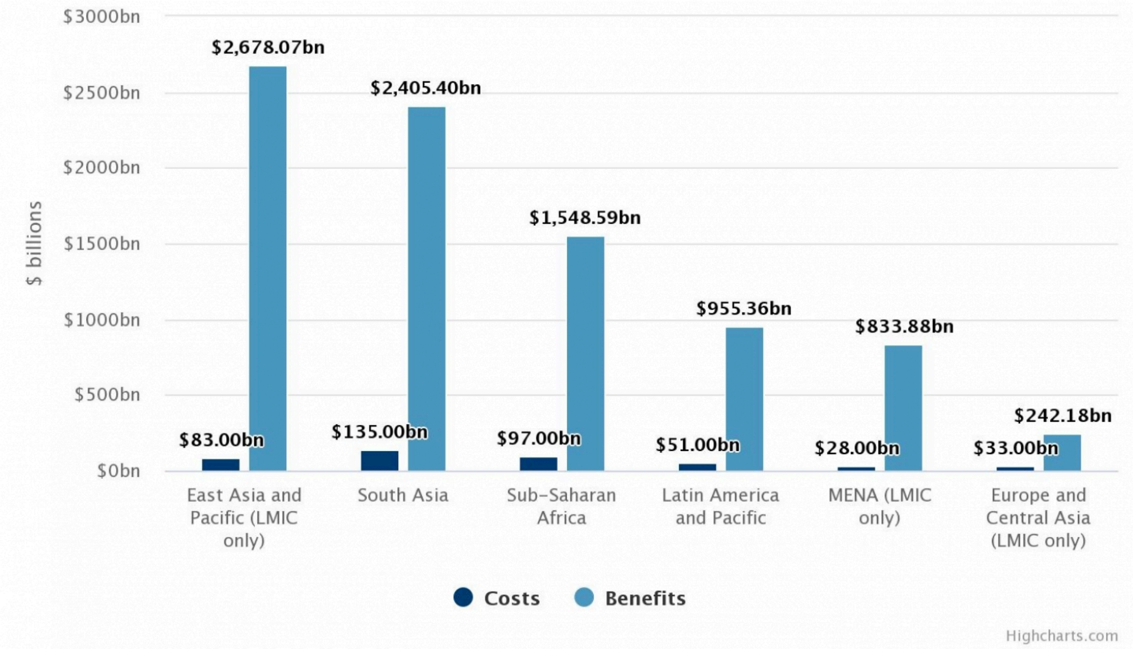
	Principle	Reasoning	Application to Internet Internationalism
Cooperation	Reserve space to cooperate with China to benefit the global commons and ensure long-term stability	China is a major power and a key decision-maker in global affairs Cooperating with China is critical to addressing key transnational challenges	Internet infrastructure in Africa Technology supply chains (for example, semiconductors and submarine cables)

Competition	Preserve the West’s competitive edge in technology and innovation	Technology and innovation can generate economic prosperity domestically as well as geopolitical leverage internationally Attracting the best talent internationally can also generate strong soft power culturally	Protecting multi-stakeholder bodies and resisting authoritarian technical standards New semiconductor foundries Investment in access infrastructure such as 6G
Confrontation	Speak out against China’s human-rights violations domestically and growing international aggression	Protect the international community’s norms, interests and values	Cybercrime and warfare Authoritarian technologies, for instance, surveillance and repression tools used domestically and exported internationally

Source: TBI

Chief among the cooperation priorities is improving internet connectivity in Africa. Not only is closing the digital divide a moral obligation, it is also in the interests of every country in the world to expand the global internet economy. It would also only cost 0.02% of OECD countries’ annual Gross National Income (GNI).

Figure 13 – Economic benefit versus cost of achieving universal internet access by region (excluding devices)



Source: The Progressive Case For Universal Internet Access, TBI

The US, EU and others cannot force China out of this market or broader governance fora entirely, and nor do they want to or need to. While managing China's growing influence is necessary, trying to isolate it entirely would put at risk other areas of cooperation or investment that China could provide. The goal should therefore be about making the market for infrastructure financing more competitive, rather than simply treating emerging economy infrastructure as a proxy battle. Establishing a foothold could also give liberal states insight into infrastructure projects and provide some challenge as well as an alternative option to low- and middle-income countries concerned about technologies provided by Chinese companies.

Charts created with Highcharts unless otherwise credited.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Renewing Domestic and Global Institutions

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- In the face of authoritarian challengers and growing technological complexity, traditional internet-governance institutions are failing to maintain, coordinate and promote the open internet model that generates so much economic and social value.
- Debates over standards such as DNS-over-HTTPS and China's New IP proposal illustrate how technical fora are increasingly making global policy decisions for which they are ill-equipped.
- Tech-diplomacy initiatives have grown in recent years, with leading countries using this as a new avenue to shape the geopolitical role of the tech industry and integrate digital and technology issues into foreign policy.

If geopolitical incentives are failing to promote effective cooperation between key states such as the US and EU, what about institutions? Unfortunately, both domestic governments and international bodies are increasingly ill-equipped to deal with a governance environment that is becoming more and more complex. While the internet itself has developed rapidly, now evolving into new fields such as the "internet of things" and decentralised networks, the institutions of the Web 1.0 era are unprepared for being used as instruments of geopolitical ambition.

Notably, there is wide consensus within internet-governance communities – be it from technical participants, national policymakers or industry players – that the current institutional model is broken. But reform is costly and time-consuming, even if all could agree on a new model. To provide a common understanding of these challenges, this section sets out how these institutions are broken and why reform is so hard.

Internationally, today's organisations have strengths that should not be disregarded, but the whole governance ecosystem needs significant overhaul to be effective in this more complex environment. At a domestic level, states also need to treat internet governance as a foreign-policy priority and adopt a coherent strategy that integrates existing programmes, domestic regulations and new forms of cooperation.

International Institutions

As we set out earlier, there are several international institutions focused on developing and maintaining the technical aspects of the internet including security standards and communication protocols. In theory, anyone with a technically sound argument can participate in these discussions and decisions are made by consensus. The market then acts as a selection mechanism: if technological proposals are good and useful, they will be adopted; if not, they won't. These characteristics combine to make up the "open, multi-stakeholder" model of governance that has enabled the internet's extraordinary growth.

However, these institutions were also never designed to cope with the machinations of geopolitical competition and an increasingly complex internet ecosystem. Organisations such as the International Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) represented the hope and optimism of the early internet, led by technical communities but with representation from civil society and some government actors. Yet many of these institutions are now falling short of what's necessary.

The most challenging issues are the lack of policy capability, authority and global representation of governance bodies. The lack of authority, in particular, enables geopolitical aggressors to go "forum shopping": making proposals to multiple bodies in the hope they are taken up by at least one. This is an important constraint on the ability of today's institutions to counter growing (geo)politicisation.

Lack of Policy Representation

Technical institutions have always embedded internet values, be they focused on privacy, security or openness. But technical decisions increasingly have significant consequences for policy, and states are limited in how they can shape these discussions. Indeed, forum participants with significant market power can both submit standards proposals and choose to implement those standards in services with billions of users. As such, there can be very little opportunity for states or civil society to intervene or raise policy concerns about these technologies.

Case Study: DNS Over HTTPS (DoH)

One recent example of the lack of policy representation in technical fora is that of DNS over HTTPS (DoH), a proposal which was developed at the IETF by a working group chaired by a representative from Google.

The context for this proposal is Edward Snowden's leaks about the surveillance of global internet activity by Western intelligence services. One technique that underpinned this was to intercept unencrypted DNS requests, which convert strings of text like "en.wikipedia.org" into an IP address like 208.80.154.224. In response, participants of the IETF proposed a new standard that would encrypt these requests at source to protect users' privacy, stopping anyone from using this technique to inspect browsing activity.

This approach, DNS over HTTPS (DoH), has now been implemented in many leading browsers, including Google Chrome and Firefox. Apple has also recently released Private Relay, a feature that encrypts traffic leaving a user's device and routes it through multiple other internet relays, so that no one, including Apple, can see a user's browsing activity. For intelligence agencies in the US, UK and elsewhere that have relied on this vulnerability for surveillance, including to identify illegal content such as terrorist and child exploitation and sexual abuse (CESA) material, these steps have created a problem.

These technologies have significant benefits for user privacy. Whatever their merits, however, by undermining this technique and domestic policy lever, a technical forum on privacy – together with private actors who have commercial incentives – have set global policy without a wider public discussion of the associated trade-offs for online safety or democratic legitimacy.

In general, IETF and other bodies' commitment to non-prescriptive protocols ensures that the internet's underlying architecture is secure, effective and free from political interference. The IETF should not be burdened with the weight of geopolitical policy, and the internet would not benefit by reactively intervening more directly in these fora, since preserving the neutrality of infrastructure lower down the stack is important.

Nevertheless, it is also true that the status quo of policy decisions made in fora that cannot envisage, and are not accountable for, their full political ramifications is not sustainable. Unfortunately, the Internet Governance Forum (IGF), which is supposed to promote dialogue on these global internet policy decisions, also lacks the necessary authority to step in.

Lack of Authority and Global Representation

The IGF, a UN-affiliated organisation set up to promote global dialogue on internet policy and governance, lacks any real decision-making power. As such, it is routinely viewed as little more than a "talking shop" by both the biggest technology companies and nation states alike, weakening its relevance. Similarly, while the IETF and W3C are well-respected standards organisations, they are frequently competing for responsibilities with the International Telecommunication Union (ITU), another UN body, which undermines its authority.

> #### Case Study: China's New IP at the ITU vs IPv6 at the IETF
>
> As participatory models that favour a free and open internet undermine the influence of countries with alternative objectives, authoritarian states are increasingly turning to UN-affiliated organisations with greater authority such as the ITU for standards-setting.
>
> For example, as the number of internet-connected devices worldwide grows, the current IP address system – IPv4 – will run out of addresses. The IETF, which is primarily responsible for internet standards, has proposed a new system called IPv6. However, China has used the ITU to promote its competing New IP proposal, *after* it was originally rejected at the IETF and elsewhere.
>
> This battle is a microcosm of the more assertive steps on standards and infrastructure that the ITU has been taking since 2012, following the World Conference on International Telecommunications 2012 (WCIT-12), which expanded the ITU's mandate beyond telecommunications to encompass the internet. This move was criticised by the European Parliament, the US House of Representatives, the Electronic Frontier Foundation, Google and others as a land grab by the UN at the expense of the existing multi-stakeholder model.

Although the IETF and similar bodies are nominally open fora, in reality they have very high barriers to entry in terms of time, resources and technical expertise required to participate. In contrast, the IGF and ITU are among the few fora where the global internet community, and particularly those from under-represented countries, have a voice. This is one variable where the dominant multi-stakeholder model is falling short.

However, voting rights at the ITU, a UN body, are only available to member states. While industry, civil society and the technical community can participate – for example, China's New IP proposal was ultimately submitted by a group containing private (Huawei) and state-owned companies (China Mobile, China Unicom) as well as the Ministry of Industry and Information Technology – decisions are led by states. As such, despite its strong global representation, empowering the ITU further risks enabling more attempts to co-opt standards settings for geopolitical objectives at the expense of the wider internet ecosystem. Indeed, China's New IP proposal was originally rejected at the open, multi-stakeholder IETF, but was taken up by the ITU – most likely due to the stronger influence China had there. This illustrates how co-opting standards decisions into geopolitical fora can undermine the quality-assurance role of a market-led, standards-setting culture.

Figure 14 – Key council working groups at the ITU favour states with less liberal internet models

ITU Leadership

Chair: China (Secretary General)

Vice-chairs:

UK (Deputy Secretary General)

Internet Policy

Chair: Saudi Arabia

Vice-chairs:

South Africa
Paraguay
UAE
India
Azerbaijan
UK

International Telecommunication Regulations

Chair: Zambia

Vice-chairs:

Ivory Coast
Canada
Egypt
China
Russia
Netherlands

SDGs and annual *World Summit on Information Society*

Chair: Russia

Vice-chairs:

Rwanda
Brazil
Saudi Arabia
Iran
Azerbaijan
Poland

The Six Official (UN) Languages

Chair: Tunisia

Vice-chairs:

USA
Kuwait
China
Russia
Spain
France

Child Online Protection

Chair: UAE

Vice-chairs:

Nigeria
Disney (sole corporate member)
Jordan
India
Azerbaijan
Italy

ITU Financial & Human Resources

Chair: United States

Vice-chairs:

Senegal
Bahamas
UAE
India
Russia
Czech Republic

Cost recovery for Satellite Networks

Chair: Russia

Vice-chairs:

Egypt
USA
Saudi
China
Kazakhstan
Romania

Strategic & Financial Plans for 2024-2027

Chair: France

Vice-chairs:

Kenya
USA
Kuwait
China
Russia
UK

Informal Expert Group on annual World Telecommunications Policy Forum

Chair: Italy

Source: ITU

The Impact of Failing Global Institutions

The lack of effective, global internet institutions has forced global technology policy to be increasingly decided in sub-standard fora. For example, Mark Nottingham, the co-chair of the IETF HTTP Working Group, has argued that regulators in the UK and US are becoming de facto internet-governance institutions by setting or overseeing the implementation of privacy, ad tracking or interoperability standards by large technology companies. These regulators are acting without any of the constraints of the community and consensus-based governance model, and all the incentives of national regulators (which tend towards divergence or power-hoarding).

Some discussions have also been pushed into "minilateral" trade negotiations, rather than being agreed at a higher or global level. The US, for example, used the United States-Mexico-Canada Agreement (USMCA) to enshrine liability protections for technology services internationally, akin to its domestic Section 230 law that limits intermediary liabilities. This would also likely affect UK plans for an Online Safety Bill, if the US and UK were to begin trade negotiations. Putting the merits of Section 230 aside, bilateral trade agreements are a poor way to achieve alignment on technology regulations with global impact.

Prospects For Reform

While there is wide consensus that many internet governance fora are broken, reform is challenging because:

- The time and costs involved in a sufficiently radical reform process make achieving a successful outcome very hard
- Broader geopolitical tensions may undermine agreement on a new proposal
- Existing institutions have strengths and expertise that are critical to the working of the internet ecosystem, and which should not be lost in the process
- Many nation-states are already over-extended, leading to reluctance to create any new fora that might duplicate existing discussions.

One promising idea has come from a recent consultation led by the UK–China Global Issues Dialogue Centre at Jesus College, University of Cambridge. This proposed a new ecosystem oversight body modelled on the Intergovernmental Panel on Climate Change (IPCC). Like the IPCC, this would leverage technical expertise from across governments, industry and civil society to increase transparency and common understanding of the issues, threats and opportunities, as well as the specific threats facing the global internet. Given this early-warning system does not yet properly exist, and thus would not duplicate any existing institutions, establishing an "IPCC for the internet" would be a no-regrets move.

For advocates of broader institutional reform, the IGF is a cautionary tale. Established in 2006, it was supposed to be the new institution that resolved the governance challenges of the day. However, in recognition that it has fallen short of promoting action over debate, diplomatic momentum is now building behind the UN's 2020 Roadmap on Digital Cooperation proposal of a new "Internet Governance Forum Plus" (IGF+) model. This would include:

- Formal anchoring of the IGF within the UN, with responsibility for the IGF moved to the office of the UN secretary general
- New organisational units including an advisory group, cooperation accelerator, policy incubator, and an observatory and help desk. With membership coming from industry, government and civil society, these units intend to promote actionable outcomes by coordinating with, and feeding into, other key governance bodies.
- A new IGF trust fund to promote financial sustainability. This would be a voluntary funding mechanism, with governments, international organisations, businesses and the tech sector encouraged to sustainably support the IGF for the long-term.

Support has been building for this proposal, with the European Commission's Executive Vice President Margrethe Vestager recently calling for a revamped IGF. By seeking to address the lack of policy capability in particular, if the new model can live up to expectations then the internet ecosystem will certainly be better off. These reforms would also be consistent with the results of the 2020 *We, The Internet* global citizens dialogue, which indicated strong support for a multi-stakeholder and global approach in internet governance among global internet users. However, given that the most geopolitically important technology companies have traditionally taken minimal heed of the IGF, even a reformed version would have a long way to go to establish its authority.

Figure 15 – Key institutions today fall short on representation and policy, creating a critical governance gap

	Standards bodies (e.g. IETF, W3C)	"Minilaterals" (e.g. G7, Five Eyes)	ITU (UN)	IGF (UN)	IGF+ (UN)
Technical Expertise	✓	⋯	⋯	⋯	⋯
Policy Capability	✗	✓	⋯	⋯	⋯
Global Representation	✗	✗	✓	✓	✓
Effective Structures and Cultures	⋯	✓	✗	✗	⋯
Authoritative	✓	⋯	✗	✗	✗
Reliable Funding	✓	✓	✗	✗	⋯

Key:

✗ No

⋯ Uncertain

✓ Yes

Source: TBI summary of analysis and expert interviews

Domestic Capability

Domestic state capacity also matters because many government departments – from cybersecurity and military agencies to ministries focused on foreign and digital policy – have a stake in shaping both national regulations and international cooperation.

Some states, such as the UK, have the necessary expertise to promote their interests in the international institutions that govern the internet ecosystem. But all too often, this expertise either isn't empowered to shape decision-making or is not connected with other work across government. This is both a structural and a strategic problem.

On the structural, elsewhere we have made the case that countries should have an integrated Digital, Data and Technology Department to better align digital policy and delivery. However, in global internet governance and geopolitics, there are foreign-policy aspects that even this department could not reasonably manage. The internet has created new global power dynamics and new types of conflicts while challenging norms around sovereignty and the liberal idea of global interdependence. It is therefore the responsibility of foreign ministries to articulate a comprehensive, coherent and holistic strategy that grasps this new context, articulates priorities, and resolves the clashes that arise between traditionally siloed government departments.

To that end, countries including Denmark, Australia, France, Switzerland and the Netherlands have all designed digital foreign-policy strategies to take a more holistic approach to the intersection of tech and foreign-policy objectives. This has included creating new diplomatic structures such as tech ambassadors, improving skills, ensuring collaboration between national government departments and promoting multi-stakeholder initiatives.

TBI analysis has identified 27 jurisdictions (including the EU) that have established some form of tech-diplomacy initiative to varying degrees of maturity. (In November 2019, the UAE also announced plans to establish an Ambassador for the Fourth Industrial Revolution but the status of this is currently unclear so it is excluded from the list below.)

Figure 16 – Global tech-diplomacy initiatives

Country or territory	Tech diplomat	Dedicated foreign affairs entity	Dedicated strategy	Notes
Australia	Yes	Yes	Yes	-
Denmark	Yes	Yes	Yes	-
Estonia	Yes	Yes	Yes	Estonia's foreign policy strategy contains a Digital Agenda, including a Cybersecurity Strategy.
Germany	Yes	Yes	Yes	Cyber Foreign Policy Coordination Unit set up in Federal Foreign Office in 2011.
Switzerland	Yes	Yes	Yes	-
Austria	Yes	Yes	No	-
Canada	Yes	Yes	No	Unit in Global Affairs Canada is focused mainly on cyber security, but SF Consul General is a 'digital diplomat'.

Country or territory	Tech diplomat	Dedicated foreign affairs entity	Dedicated strategy	Notes
Czech Republic	Yes	Yes	No	Special Envoy and his unit in MOFA is focused on cyber security
China	Yes	No	Yes	PRC embassies and consulates in 52 countries have 'science and technology diplomats'
France	Yes	No	Yes	-
Finland	Yes	No	No	Has a cyber security strategy with minor international aspects. Ambassador focused on security
Hungary	Yes	No	No	-
Kazakhstan	Yes	No	No	-
Lithuania	Yes	No	No	-
Malta	Yes	No	No	-

Country or territory	Tech diplomat	Dedicated foreign affairs entity	Dedicated strategy	Notes
Portugal	Yes	No	No	-
Slovenia	Yes	No	No	-
United Kingdom	Yes	No	No	-
Israel	Yes	No	No	
USA	Planned	Planned	No	Government is planning on establishing Bureau of Cyberspace Security and Emerging Technologies. Will be headed by Ambassador-at-Large.
EU	Planned	No	Planned	Estonia, France, Germany, Poland, Portugal and Slovenia produced a non-paper with proposals for EU's future cyber diplomacy.
India	No	Yes	No	New Emerging and Strategic Technologies (NEST) Division set up in January 2020.

Country or territory	Tech diplomat	Dedicated foreign affairs entity	Dedicated strategy	Notes
Japan	No	Yes	No	Entity is the Advisoy Board for the promotion of Science and Technology Diplomacy.
Netherlands	No	No	Yes	Start-up liaison personnel based in Silicon Valley, but excluded given that it is not a formal diplomatic position or outpost.
Norway	No	No	Yes	-
Spain	No	No	Planned	Strategy under development. "National Technology and Global Order Strategy will diagnose the role of technology in power relations between States with an effect on conditions of progress and society as a whole."
Ethiopia	No	Yes	No	

Source: TBI

Crucially, this capability is as much about enabling states to stop initiatives not in their interests as it is about promoting positive initiatives. For example, Russia is currently working to move responsibility for cybercrime from the Council of Europe to the UN, while China would like the ITU to play a greater role in internet governance at the expense of industry-led technical forums that favour the West. Both of these steps would disempower institutions that support Western values, but resistance will fall short without effective state capacity.

An integrated strategy, which takes technology policy seriously as a foreign-policy priority, can provide a guiding framework that empowers different teams within governments to look ahead and identify capabilities that are missing or will be in demand. It would also highlight whether technical representatives in global governance fora are sufficiently well-equipped to take on geopolitical debates, and where like-minded allies can cooperate to stabilise the internet ecosystem.

Charts created with Highcharts unless otherwise credited.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: China, Emerging Economies and the Spread of the Authoritarian Model

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- China has developed an effective strategy to export its domestic internet model, which combines standards, domestic regulations and international infrastructure financing designed to expand the influence of its tech champions globally.
- So far, the US, EU and other D10 countries have done little to resist this strategy. Infrastructure offerings from these countries have become uncompetitively slow and expensive – leaving little room for low- and middle-income countries (LMICs) to make decisions based solely on the values they prefer.
- With 3.7 billion people still without internet access, LMICs will come to play an increasingly important role in internet geopolitics. But they face a tipping point in deciding which internet model to pursue: for many leaders grappling with fragile development pathways, demographic challenges and minimal digital economies, the internet is seen more as a source of social disruption than economic growth.
- LMICs working to leapfrog legacy systems and deliver more effectively, however, must adopt technology infrastructures and policy frameworks that support open innovation, rather than curtailing it.

While liberal democracies have turned inwards, stepping back from global leadership on internet policy, China has come forward. It has been able to execute a strategy to expand its global influence and export its domestic, authoritarian internet model that, from its perspective, is entirely rational and coherent. Unfortunately, it has faced little opposition in the process.

China's Authoritarian Playbook

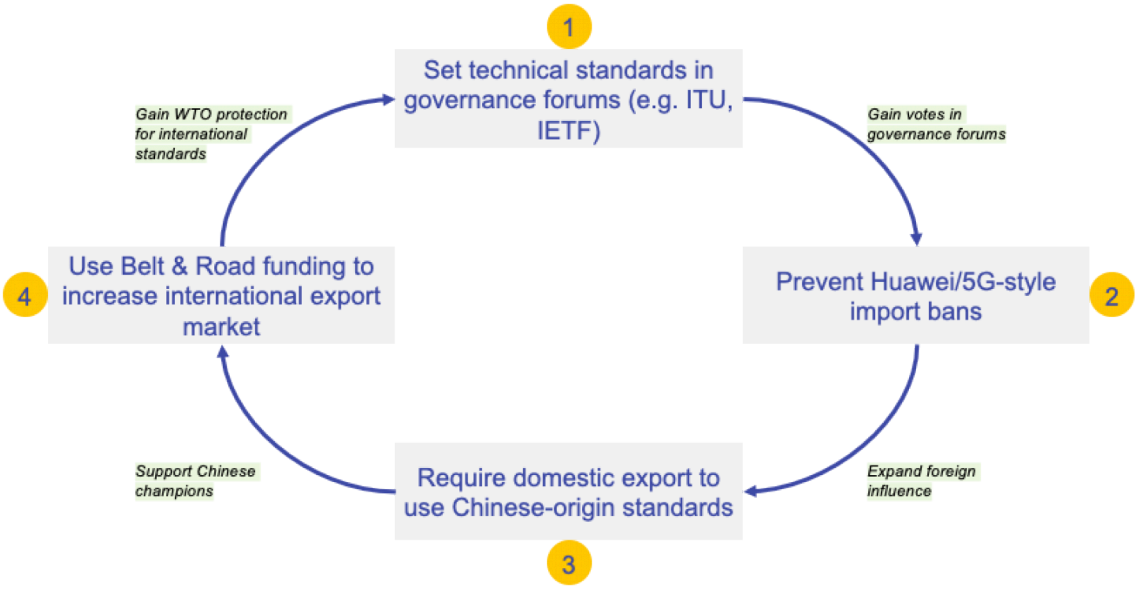
The growth of China's digital economy may have initially been defined by imitation – with key domestic champions protected by the government as they adopted insights from Western firms – but today innovation and investment are its key characteristics. China is now taking an increasingly active role in technical-standards bodies and promoting New IP, AI, smart cities and facial-recognition tools. In the process, it is abusing the principle of digital sovereignty to allow states to break the internet's fundamental openness.

Given that the internet's distributed "network of networks" architecture acts as a selection mechanism, actors such as China have limited ability to impose changes from the top down. However, standards do still matter even if they are not adopted globally. As Dominique Lazanski, Stacie Hoffman and Emily

Taylor set out in the *Journal of Cyber Policy*, standards agreed in governance fora such as the International Telecommunication Union (ITU) gain international protections via the World Trade Organisation, which can help China avoid bans on importing technologies from its domestic champions (e.g. Huawei). It is also able to internationalise its domestic technologies via infrastructure projects that are part of the Belt and Road Initiative including, for example, the requirement that domestic exports use Chinese-origin standards.

While China has not set out an explicit, publicly available description of its international strategy, we can piece together the evidence above to describe a repeatable playbook on internet standards and infrastructure, as set out below:

Figure 17 – China has been executing a long-term strategy on technical standards and internet infrastructure


1
Set technical standards in governance forums (e.g. ITU, IETF)
Gain votes in governance forums
2
Prevent Huawei/5G-style import bans
Expand foreign influence
3
Require domestic export to use Chinese-origin standards
Support Chinese champions
4
Use Belt & Road funding to increase international export market
Gain WTO protection for international standards

Source: TBI adaptation from strategies identified in Standardising the Splinternet

Why a Progressive Response Matters

So far, the US, EU and G7 nations – plus any others that would support an open, liberal internet model – have had no comparable strategy to China's approach. While recent steps towards transatlantic tech cooperation offer grounds for cautious optimism, it remains a long way from a comprehensive strategy.

As this develops, many advocates of internet freedom are concerned about geopolitics co-opting internet governance even further. Indeed, the global internet will not be well-served by the US and others imitating China's level of interventionism, but as a geopolitical contest is no longer avoidable, liberal democracies must face up to the challenge.

What's clear is that the next step must be proactive and competitive on the merits – cost, speed, and minimal bureaucracy – rather than reliant on minimalist containment strategies. For example, US sanctions on Iran prevented GitHub, a US software company rooted in internet openness, from making its services available to developers there. Meanwhile, China stepped in to establish a partnership based on improving technology infrastructure and capability. Hostility between the US and Iran goes far deeper than a particular set of sanctions, and Iran makes it hard for US companies to operate in Iran anyway. However, this case indicates the limits of a containment approach against internet authoritarianism, given China's willingness to step in. This lesson will be important in deciding how to support the growth of an open internet model among the large group of non-aligned states – the so-called Group of 77 (now actually 134 countries) – which are at a tipping point in deciding which path to follow. To win the race for the future of the internet, liberal countries will need to compete – and make the case – on the merits.

Emerging Economies Trending Towards Restrictive Models

Currently, 3.7 billion people around the world have no access to the internet. This means developing countries will play an increasingly important role in shaping internet governance and geopolitics in years to come. Yet, on the present trajectory, LMICs seeking to build this connectivity are likely to access the necessary financing from China rather than the US, EU or affiliated development organisations.

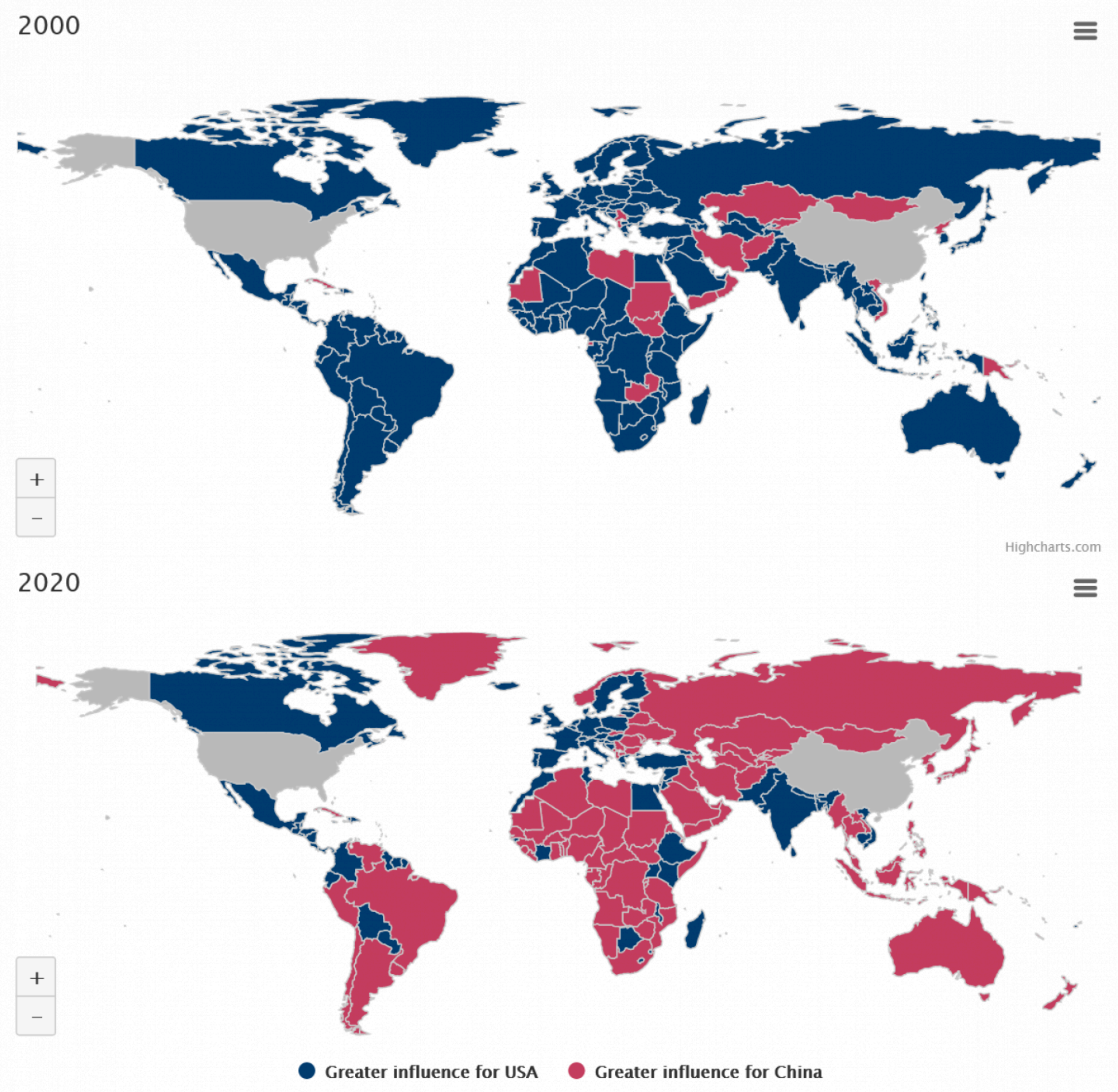
Through the Digital Silk Road (DSR) component of its Belt and Road initiative (BRI), China has become a valuable partner to emerging economies seeking technology-infrastructure financing and support. While its overseas lending has been scaled back since 2018, between 2008 and 2019 a total of $462 billion had been lent overseas by just two state-controlled Chinese banks – the China Development Bank and the Export-Import Bank of China. Of this, an estimated $79 billion has been committed to Digital Silk Road projects globally.

The Significance of Infrastructure Support

Meanwhile, Western infrastructure support has become uncompetitively slow and expensive, especially in Africa, the last frontier for the internet. As we have set out previously, development programmes run by organisations such as the World Bank and International Monetary Fund (IMF) are often too bureaucratic and risk-averse for African governments trying to create jobs quickly, given "youth bulges" (large increases in the proportion of a population's youth) and risks of manufacturing automation.

As such, even if China's loan terms may pose some long-term risks, if it is the only partner willing to provide such affordable financing, then choices about values are secondary – even for those African countries that may be sympathetic to liberal norms. Recent G7 announcements of a Build Back Better World (B3W) initiative indicate some ambition here, but they fall short of an effective, practical plan with financial commitments on the scale required.

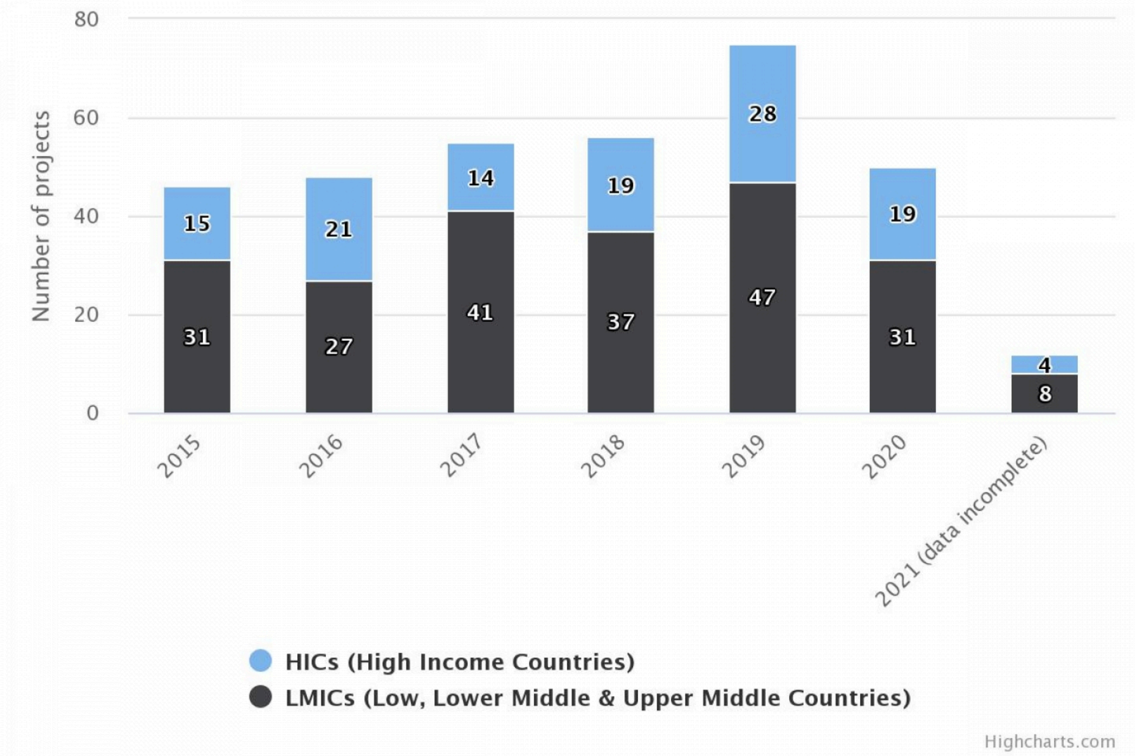
Figure 18 – China has overtaken the US as a trade partner across the world, measured by global imports, 2000 vs 2020



Source: *IMF Direction of Trade Stats*

While China's economic contribution to global internet connectivity should not be overplayed as an existential threat to liberal countries, it is worth noting that the country has also sought to use this infrastructure support in order to further its geopolitical aims. Indeed, as set out previously, it is executing a long-term, coherent strategy to expand its influence via standards bodies and infrastructure projects financed via the Digital Silk Road. The criticism that China is using the BRI to create client states can be overblown, but Beijing is using this route to open new markets while, at the same time, expanding the global influence of its domestic tech giants such as Huawei.

Figure 19 – Huawei's pitch is still finding success globally, despite US ban in May 2019



Source: Australian Strategic Policy Institute (ASPI) – International Cyber Policy Centre (Although there is a drop in recorded global Huawei projects in 2020, due to the coronavirus economic shock it is not possible to attribute this solely to the US's May 2019 ban. Chart also only includes projects categorised by ASPI as: cable; cable terrestrial; R&D lab; telecommunications or ICT; facial recognition; data centre; 5G relationship; manufacturing facility; "Smart City" public security project; health; and surveillance equipment. All projects with missing data for "year commenced" also excluded)

Digital Silk Road and Expanding Authoritarianism

While the attraction of these deals is often about cheap financing for much-needed infrastructure, these projects can also present significant national-security risks and enable relationships where China is dominant.

For example, in 2018, the African Union (AU) accused China of hacking the IT systems at its headquarters in Addis Ababa, Ethiopia. For five years, every night between midnight and 2am, data from the AU's servers had reportedly been transferred to Shanghai while listening devices were also allegedly found during a security sweep. The AU's headquarters had been funded by China and built by a Chinese state-owned constructor while Huawei had supplied the IT system. Despite this, Huawei and the African Union renewed their relationship in 2019, possibly reflecting China's dominance in the relationship.

For the international community, there are also concerns that infrastructure projects may enable leaders to impose greater censorship and shutdowns – or even technically decouple from the global internet. Often part of broader "smart and safe" city initiatives, many of these projects are presented as helping states to "identify threats to public order" by using technologies such as facial recognition, CCTV and crime-monitoring systems. Similarly, China's New IP proposal – which could enable fragmented, sovereign internets with greater state censorship and surveillance – is now undergoing a pilot domestically and could then be exported internationally, potentially following the pattern of other domestic standards and technologies.

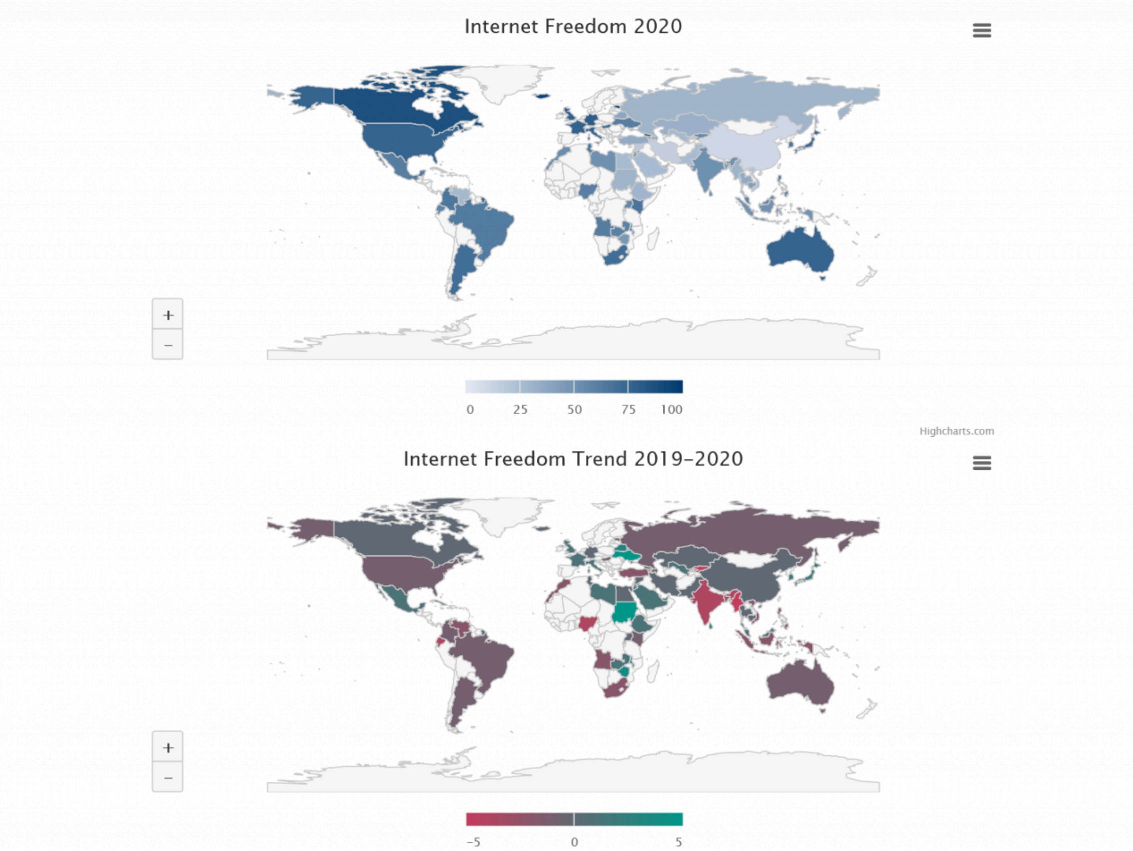
It is important to recognise that African states have as much right as any sovereign country to protect the security of their societies. Similarly, there is rarely a "smoking gun" that conclusively demonstrates the motivations of either China or its partners around the world; the technical ability to impose an internet shutdown cannot alone signal intent. International interpretations of the plans of African states are nevertheless influenced by the precedent of China's domestic internet authoritarianism, including its widespread censorship and apparent "social credit" system.

The result is that while the majority of the connected world currently benefits from a relatively free and interoperable internet, there is a very high risk that, as the rest of the world becomes connected, it will experience a much more restrictive internet model. In closing one digital divide, another may open: between those who can meaningfully access the internet's freedoms and opportunities, and those who cannot.

A New Digital Divide Beyond Access

On current trends, many emerging economies globally are moving towards a restrictive internet model, as shown by data from Freedom House. In Africa, only South Africa is listed as “free” according to an “internet-freedom” score, though the limited data set – with some notable omissions – constrains the story that can be told about the continent.

Figure 20 – Scoring internet freedoms globally



Source: Freedom House

Given its perceived limited benefit, and growing capacity for disruption, the internet sector in many emerging countries does not get the political protection it warrants over the long term from an economic point of view. Rather, the internet in emerging countries is often subject to shutdowns and disproportionate restrictions. The recent impasse between Nigeria’s government and Twitter is indicative of this.

Case Study: Nigeria's Twitter Ban

On 4 June 2021, Nigeria's government announced an indefinite suspension of Twitter's operations in the country, citing "the persistent use of the platform for activities that are capable of undermining Nigeria's corporate existence." The suspension was announced just two days after the platform deleted a tweet by President Buhari for violating its rules.

The president's tweet referred to the Nigerian (Biafran) civil war in a threat to deal with those "misbehaving today in... a language they will understand". In the few weeks leading up to the ban, authorities accused banned separatists of attacks on electoral offices and prisons in southeast Nigeria. Nigeria's minister of information said Twitter had not banned incitement tweets from other groups.

On 5 June, the Association of Licensed Telecommunications Operators disclosed a directive from the industry regulator to suspend access to Twitter. On 6 June, Nigeria's National Broadcasting Commission (NBC) directed all TV and radio stations to "de-install" and desist from using Twitter, describing the activity as "unpatriotic". The government also directed the NBC to immediately commence the process of licensing all perceived over-the-top (OTT) and social-media operations in what will set the stage for further regulation.

Nigeria has the highest reported number of internet users in Africa. Many of the country's Twitter users have resorted to virtual private networks (VPNs) to access the platform where they are amplifying the call to revoke the ban by leveraging the global open internet #KeepItOn campaign. Although Nigeria's attorney general originally vowed to prosecute those violating the directive, he has since walked back from these comments. Analysis by Top10VPN estimates that the country's ban affected around 104.4 million internet users and cost Nigeria $366.9 million between June and July, about $6 million a day.

Africa and the Restricted Internet

While openness and permission-less innovation have been the foundations of the Western internet, the pathway to an open internet is still contested in Africa. So long as the internet economy remains small, it is unlikely to receive political protection from shutdowns or disproportionate restrictions. Yet internet economies cannot grow sustainably without a stable, growth-oriented, rights- and freedoms-respecting regulatory regime.

So, bold political leadership is necessary to escape this catch-22. Where there has been political interest – such as in response to the Global South potentially missing out on $2.8 billion in tax revenues from Facebook, Microsoft and Alphabet, Google's parent company – the response has all too often been focused on ineffective and disincentivising tax regimes. In this scenario, Nigeria's current leading tech sector may yet pay the costs of increased political intervention.

In contrast, Ghana exemplifies the rewards of senior, political commitment to a healthier internet.

Case Study: Ghana – The Choice for Twitter's Africa HQ

On 12 April 2021, Twitter announced that it was establishing its presence in Africa with an office to be headquartered in Accra, Ghana. The decision largely came as a surprise to the general public and sparked a vigorous debate about the business ecosystem for technology start-ups across the continent.

Explaining its rationale, Twitter stated that Ghana is "a champion for democracy, a supporter of free speech, online freedom, and the Open Internet." Furthermore, Ghana's recent appointment to host the secretariat of the African Continental Free Trade Area provided additional incentive for the social-media platform looking to tailor its service across the continent.

While internet and communications technology (ICT) services only contribute about 3.6 per cent to Ghana's GDP, the country's stable, growth-focused internet regulatory environment, including not a single shutdown, provided a compelling business and geopolitical case on which Twitter could build and extend its reach in Africa.

Twitter's choice of Ghana for its expansion on the continent demonstrates how African countries with more internet users and economic might, but also greater restrictive internet policies, can end up missing out on the foreign investment needed for growth.

Reversing the Trend

Over the long term, the economic cost of domestic internet authoritarianism, and fragmented internet models globally, is immense. While most internet policy debates today are focused on narrow, visible, short-term issues, reversing these broader trends will require a much greater focus on how the underlying stability and openness of the internet is threatened in the longer term.

Advocates for internet openness in emerging economies must start by understanding leaders' priorities and frame campaigns based on those terms. Fragile development pathways, demographic challenges and small internet economies are hurdles: at best the internet might be seen as irrelevant to achieving the economic aims of leaders or, at worst, as a major barrier to social cohesion and public safety.

But the tech revolution is also enabling step changes in public services, health care, agriculture and access to markets that have turned the traditional development paradigm – Global North to Global South, incremental change, zero-sum – on its head. There is a real opportunity for states to leapfrog legacy systems and deliver far more effectively for their people than they otherwise would have. Whether they succeed will be determined by the technology infrastructure and policy frameworks they have in place – in other words, do they support this open innovation, or curtail it?

Charts created with Highcharts unless otherwise credited.

TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

The Open Internet on the Brink: Recommendations for a Future Model

ANDREW BENNETT
MELANIE GARSON
BRIDGET BOAKYE
MAX BEVERTON-PALMER
AKOS ERZSE

Key Points

- Given the cooperation challenges of internet geopolitics, we need to adopt a new mindset and build a new model of *internet internationalism*. This should integrate state-level regulation, international coordination and the interests of multiple stakeholders to protect and nurture the internet ecosystem.
- By mapping out trade-offs, emerging trends and available policy levers, we can reassess states' core interests and identify novel coalitions to make progress.
- Specifically, **D10 countries should establish a new progressive state alliance** that combines security guarantees with commitments towards an open internet; the **UN should establish a new geopolitical settlement with the global technology industry**; nations must **upgrade their foreign policy strategies**, integrating technology and the internet into traditional diplomacy; and there should be **a new ecosystem oversight body** that reports on the health of the internet to help protect its future.

Securing geopolitical and internet stability against the backdrop we have set out requires a new approach. Akin to climate change, this is considered by some a "wicked problem"; making progress demands creative, hybrid policy solutions to align an array of state and institutional actors, even while rivalry between the great powers thwarts attempts to build effective mechanisms for international coordination.

Building a Model of Internet Internationalism

In response, we propose a new model of internet internationalism, which can be constructed around a framework of trade-offs and interests in internet geopolitics, a range of potential futures, and the policy levers that would be needed to shape these futures.

Trade-offs and Core Interests in Internet Geopolitics

Focusing on geopolitical interests rather than existing positions can help solve some of the current stalemate in global technology cooperation. To date, hardened positions on individual issues, such as Huawei's role in national infrastructure or TikTok's ability to operate in the US, have been generated ad hoc rather than according to a principled, consistent framework. This siloed thinking has reduced opportunities for more creative negotiations across multiple issues and trade-offs while also setting a precedent for other states to take similarly reactive steps.

Progressive leaders committed to openness, proportionate regulation and global cooperation must balance competing goals and the potential negative externalities of any action. There are some key questions to explore:

- Do the benefits of increased government involvement in markets and standards-setting bodies outweigh the risks of co-opting more frontiers into geopolitical competition, potentially undermining the freedoms of technical fora?
- Will greater representation of emerging digital economies in decision-making, thereby increasing the legitimacy of internet-governance institutions, also make it harder to build and sustain effective, action-oriented coalitions?
- Can measures to counter China's expansion of power be balanced against the risks of isolating it and damaging vital areas of cooperation?
- How can advocates of the open internet respond to the growing geopolitical importance of emerging digital economies without treating them as pawns in a proxy digital conflict and relegating their agency and development issues?

The default response may be to tackle each of these challenges individually, but – because steps taken in one domain can have knock-on effects in several others – leaders should instead consider the linkages *between* the challenges and work holistically across these issues to identify novel solutions and bargaining agreements.

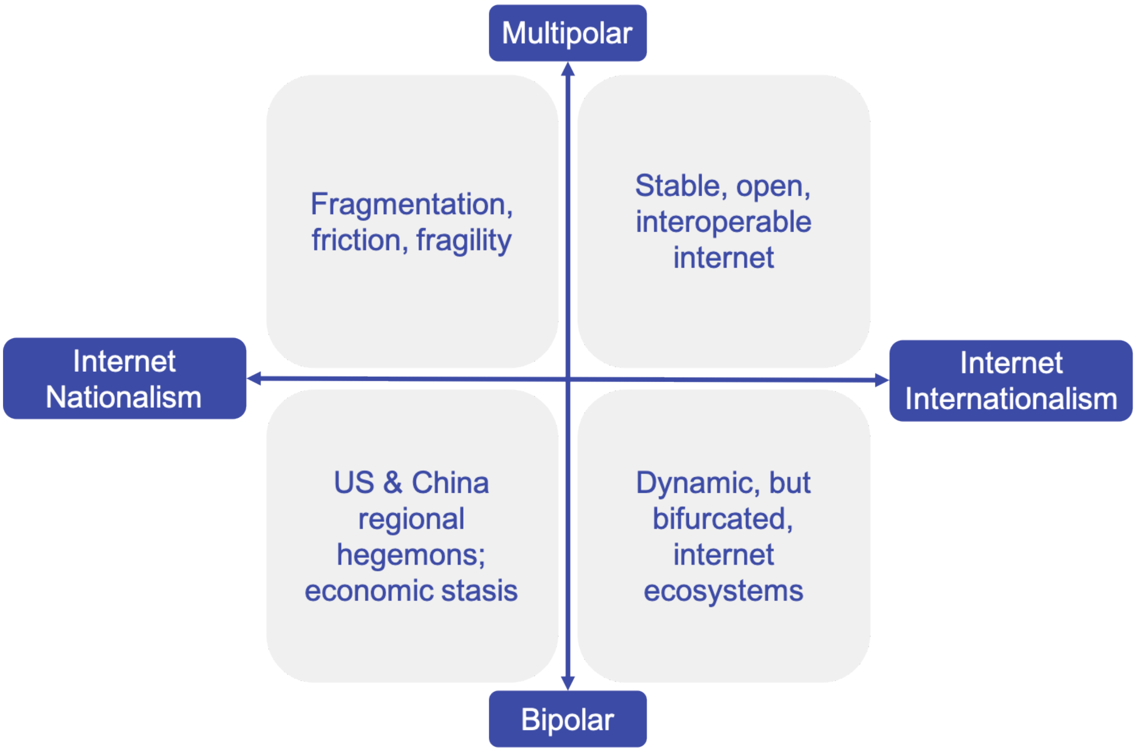
The Range of Possible Futures

To facilitate this dynamic approach to negotiation – where issues are unbundled and repackaged to find multiple, novel coalitions that can surpass a static, entrenched status quo – policymakers should consider two crucial dimensions to the future of the internet:

1. **Bipolar versus multipolar:** The tensions between the US and China may be centre stage today, but we are already moving from a bipolar to a multipolar world. This is not just about India and the EU joining the great power rivalry but about how LMICs – home to most of the 3.7 billion people who lack internet access – will come to determine the future shape of the internet.
2. **Nationalist versus internationalist:** Against this backdrop, leaders have a choice: either retreat into a more nationalistic internet strategy by prioritising sovereignty and control at the cost of long-term social and economic opportunity; or employ a strategy of internet internationalism, which recognises that building and sustaining prosperous, open and inclusive societies requires effective global cooperation. This is also the difference between an all-out cold war between the US and China or a strategic approach to engagement that distinguishes between cooperation, competition and confrontation issues.

The interplay of these dimensions could lead to many possible futures. But there is a prize to be won: an open, interoperable internet not based solely on US hegemony but stabilised through global interdependence.

Figure 21 – The future of the internet in four scenarios


Multipolar
Fragmentation, friction, fragility
Stable, open, interoperable internet
Internet Nationalism
Internet Internationalism
US & China regional hegemons; economic stasis
Dynamic, but bifurcated, internet ecosystems
Bipolar

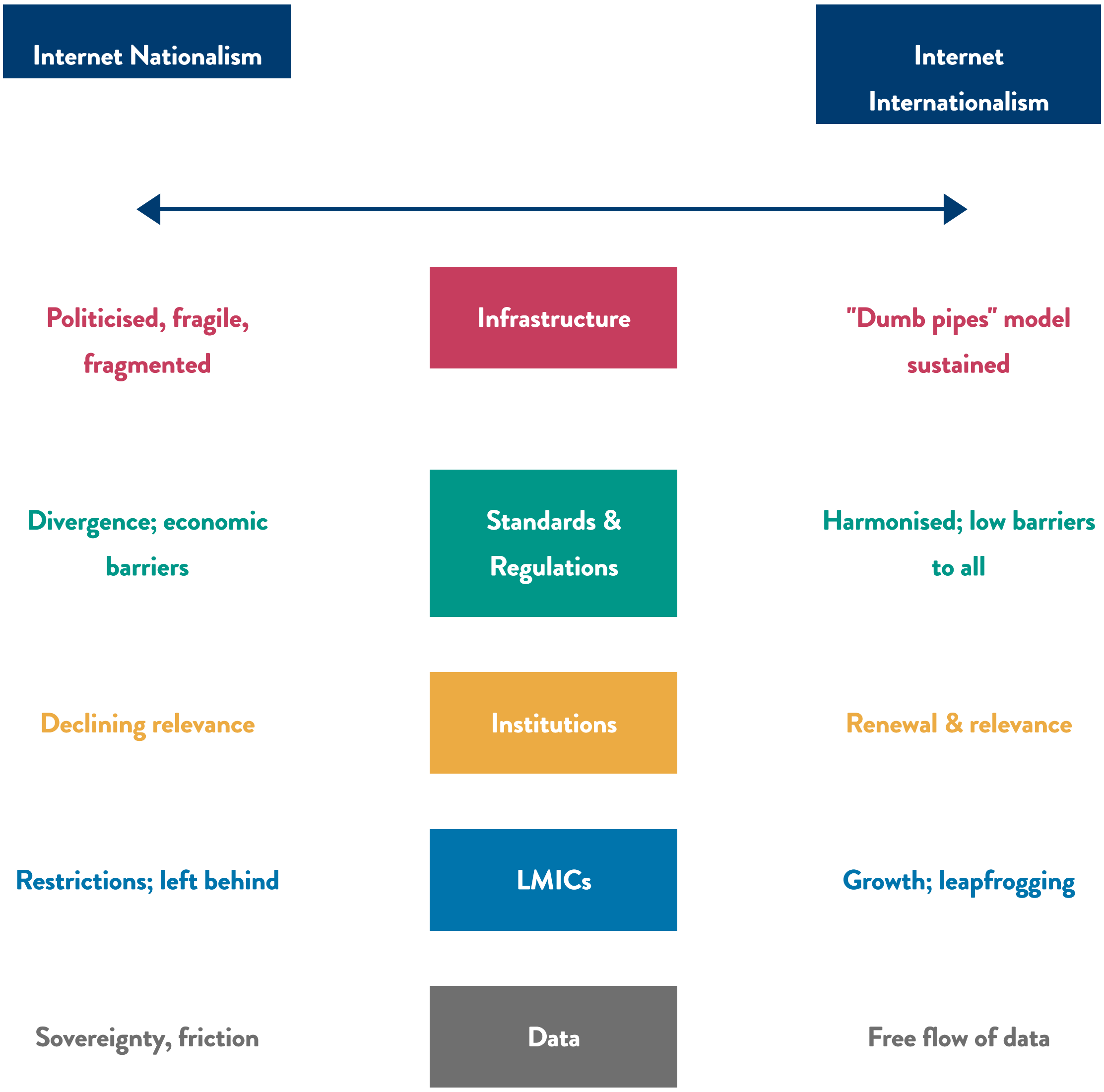
Source: TBI

The scenarios above are not mutually exclusive, and in all likelihood the balance may lie somewhere in between. However, as this report sets out, we are currently drifting closer towards a scenario characterised by fragmentation and friction than by stability and security. While some characteristics of the future will develop naturally with the evolution of the ecosystem, decisions made by the key actors in this arena are the variables that will shape these futures. Leaders have agency, and more internationalist strategies will help deliver prosperity and opportunity for all.

Policy Levers to Shape These Futures

The critical domains highlighted in this report – infrastructure, supply chains, standards and regulations – divide along a *nationalism-internationalism* axis. They are part of a continuum along which there are options for cooperation and coordination. While control and sovereignty may have short-term appeal as tools to minimise domestic social disruption or the new geopolitical power of multinational technology companies, the long-term result of tipping the balance too far is fragility, poor security, economic and social barriers, and declining relevance in the international arena.

Figure 22 – Policy levers that could shape the future

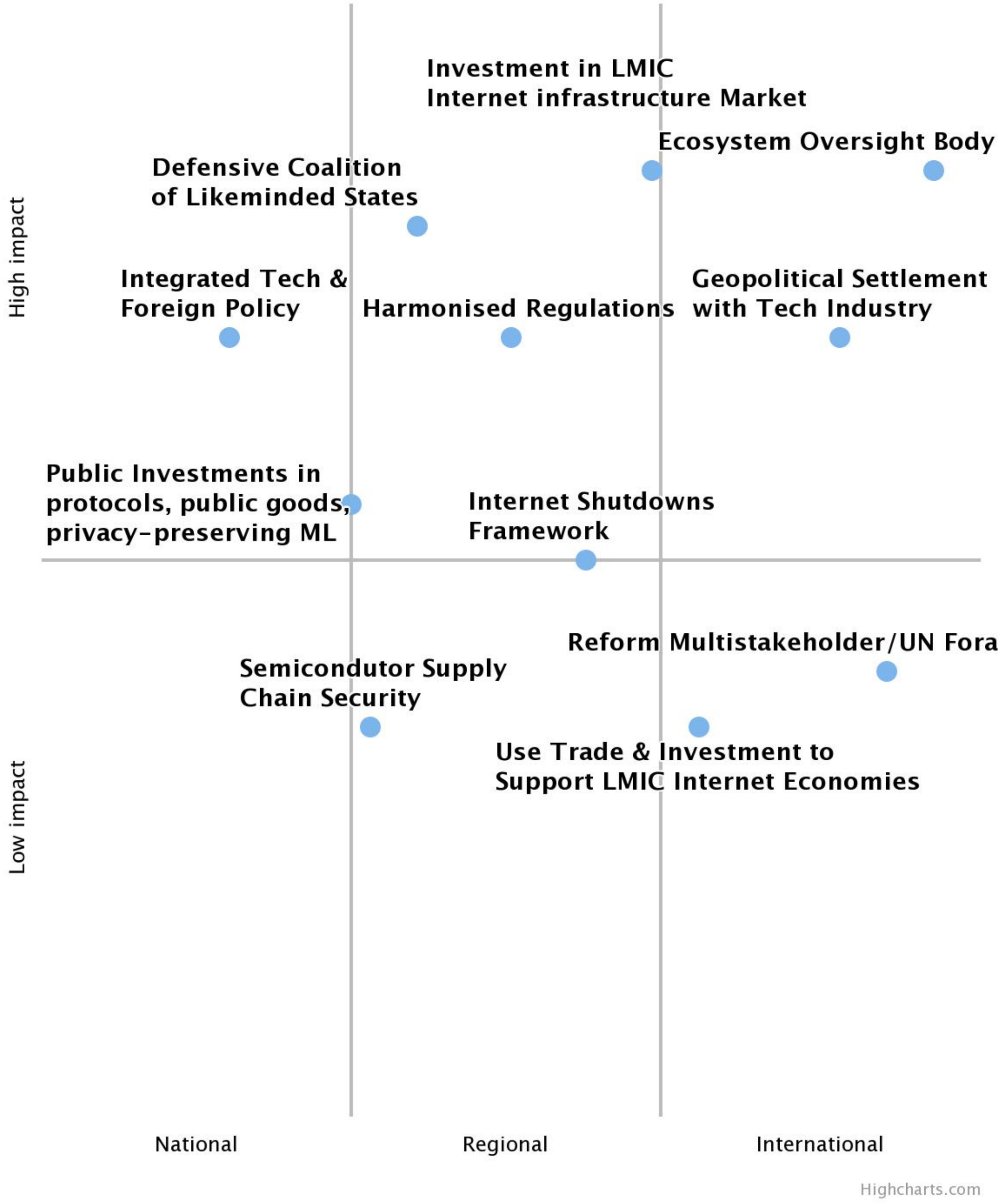


Source: TBI

Inviting all states to visualise the entire ecosystem and coordinate across a range of issues, rather than narrowly competing on a series of individual points, will allow for broader, interest-based coalitions to emerge. This provides the room for nations to be flexible on some areas such as semiconductor supply-chain security, regulatory harmonisation or internet infrastructure projects in LMICs, rather than simply picking between ideologies.

To that end, considering these key policy levers according to their prospects for global cooperation and their impact on the open internet can generate an illustrative framework to identify options and agreements for mutual gain.

Figure 23 – Illustrative mapping of policy levers, by regional cooperation and impact on the open internet



Source: TBI

This flexible approach also accommodates more security-focused strategies on issues such as semiconductors. Given that chip supply is both competitive and fixed in the short run (due to the time and cost of building new foundries), it is different to other cooperation issues such as internet infrastructure investment in LMICs where holding out for global solutions does not leave an unacceptable level of vulnerability unpatched. This approach also allows for greater transparency to understand the effects of the "hidden frontier", such as whether arguments for the onshoring of supply chains are rational against the vulnerabilities resulting from bifurcation of technical standards or global data cables. For example, in time, US and EU steps to gain more control over semiconductor supply chains may actually allow them to offer security of supply as a cooperation incentive, freeing up other states to take decisions disliked by China.

Norms of Internet Internationalism

The case for internet internationalism is compelling. However, a common focus on the clashing values and incentives of the key players in today's internet – the US, the EU, China and India; LMICs; big tech; crypto and web 3.0 innovators; multi-stakeholder forums and UN bodies – risks constraining the potential of a maximally internationalist approach. This emphasis means that areas for mutual cooperation on interests are being left undiscovered by focusing too heavily on perceptions of state interests rather than the actual problems they seek to address. Moving beyond the accepted cliché of "cooperation among like-minded democracies" would create space for unconventional actors to cooperate on issues on which they have a shared interest, as has been seen in recent US engagement with the so-called Quad countries (US, Japan, India and Australia).

Creating a new normative framework, that draws together a wider group of nations and actors in their formulation and use, will create the foundations of cooperation for internet internationalism in practice. Similar to the norms underpinning non-proliferation of nuclear weapons and the Group of Governmental Experts' (GGE) norms for uses of cyberspace, cooperation should be based on a commitment to upholding key norms and rules of law that are integral to harnessing the opportunity and prosperity of the global and interoperable internet. These norms should include commitments to:

- UN Convention on the Law of the Sea (UNCLOS) provisions on protections for submarine cables
- Commitments for transparency on uses of technologies
- Principles of international humanitarian and human rights law
- Preservation of the multi-stakeholder model for technical standards development
- Representation of, at the minimum, G7 countries in all standards fora to prevent authoritarian "forum shopping" and misuse of standards bodies.

Putting these norms together with the range of possible policy levers, we can identify four key shifts necessary to promote a progressive future for the internet at the national, regional and international levels:

- A new progressive alliance that supports the resilience of internet networks, infrastructure and supply chains and works towards regulatory harmonisation
- A new geopolitical settlement with the global technology industry

- Upgraded, nation-level foreign-policy approaches, integrating technology and the internet into traditional diplomacy
- A new ecosystem oversight body that reports on the health of global networks and internet openness, acting as an early-warning system to provide the objective, technical basis on which to measure progress.

Recommendations

1. A Digital Infrastructure and Defence Alliance (DIDA): the NATO for the Internet

The broad interconnectivity of the internet ecosystem, as demonstrated throughout this report, is both its strength and its weakness. Actors wishing to move towards internet internationalism may fear that the risks of short-term retaliatory action outweigh the long-term benefits of moving to secure the entire system. Without commitments to underpin the security of their connectivity and access to the internet ecosystem, there is no incentive to cooperate.

Building on the vision of the EU–US Trade and Technology Council – as well as similar proposals from former president of Estonia Toomas Hendrik Ilves and scholar Mauritz Kop – we are calling for a new Digital Infrastructure and Defence Alliance (DIDA). Starting with the D10 countries, this alliance could provide both the collective agreement and institutional foundation to align interests around cyber- and semiconductor-supply security, regulation and LMIC infrastructure.

Of the D10 countries (G7 plus Australia, India and South Korea), it might initially seem that India would be reluctant to sign up to commitments on internet openness. However, it may find that the security guarantees it would gain by being part of DIDA, such as on semiconductor supply, combined with its incentive to retain its status as the world's largest democracy, outweigh any other concerns. Its recent commitment as part of the Quad to secure global semiconductor supply chains indicates this is a priority strategic interest.

DIDA also recognises that, while some issues in internet internationalism should be tackled globally, there are specific issues where regional cooperation among like-minded liberal democracies can be productive. However, NATO itself is not the right mechanism: as Ilves has argued, it is focused around geography, which is less relevant in the internet ecosystem, and was not designed for a modern-day environment characterised more by digital, asymmetric attacks than in the past. In the internet era, national and cybersecurity cooperation can also be part of a greater package of collaboration including regulatory alignment, supply-chain security and global infrastructure investment rather than simply 'collective defence'.

By starting with the D10 and explicitly looking to expand further, DIDA also widens the circle of cooperation partners beyond the traditional players. To that end, the recent AUKUS announcement and new semiconductor commitments by the Quad are promising, but given their members' overlapping interests – as well as the precedent of the communiqué from the UK's G7 presidency, which included deep commitments on technology cooperation, being co-signed by the full D10 – these groupings should be expanded further.

Indeed, the long-term trajectory should be to expand the alliance to any state that is willing to commit to liberal internet values and seeks important internet-security commitments. For the LMICs that are at a tipping point in deciding their future internet model, these security guarantees would enable them to set their own internet policies without fear of retribution by any infrastructure vendors or foreign governments.

DIDA Security Agenda

A member-based DIDA would allow states to cooperate while knowing that their key infrastructure is not at risk. Modelled along the lines of a NATO alliance, partners would provide critical backup, similar to NATO Article 5, if a fellow alliance partner was subject to action affecting their connectivity or free use of the internet. For example, beyond existing cybersecurity cooperation, if a country is subject to network disruptions – either due to infrastructure controlled by another state or sabotage – the alliance could work to ensure consistent internet access, perhaps via satellite. Or if a country found its semiconductor supply cut off because it took a position in a standards institution that was not aligned with its supplier, another alliance member could step in to help bridge the gap. In this way, while EU and US attempts to gain greater control over semiconductor supply chains may appear to be a step back for open, globalised markets, they could help change their allies' cooperation incentives and thus protect the open internet in the long term. This security alliance would provide a safety net that, in turn, could allow DIDA states to act according to their best interests in technical-standards fora and other internet-governance institutions. They would be able to trade off their commitments to positions to access the opportunities of the open and interoperable internet without exposing themselves to other vulnerabilities.

DIDA Regulatory Agenda

DIDA could also enable greater international cooperation in areas such as antitrust reform, cybersecurity, data privacy, AI governance and ethics, and content moderation. While there will always be region-specific issues, it is in the interests of a productive and effective global internet economy to find areas for international alignment to prevent digital borders. This would build on the EU–US Trade and Technology Council to include wider global representation of the alliance, identifying where existing regulatory solutions can be strengthened and aligned, as well as to agree a set of common principles for future regulation. And this would include coordinating engagement in the multi-stakeholder process to develop enforceable global standards, as well as promoting the voices of LMICs, which may be disenfranchised in the setting of regulations by regulatory bodies with larger internet economies.

The DIDA initiative should also consider how coordinated public investments can shape the competitive terrain of emerging technologies such as artificial intelligence so they are compatible with liberal values. This would include aligning investment in areas such as machine-learning techniques that rely less on real-world data collection (such as simulation learning or one-shot learning). Investment to improve the viability of interpretability, fairness and privacy techniques could also shift the adoption curve within the field of AI research before path dependence sets in. A DIDA-AI research institute with ambitious public funding would be well positioned to make progress on these competitive terrain questions.

DIDA Internet Infrastructure Agenda

DIDA should also provide the support needed to coordinate a new transatlantic belt and road for the internet. While the G7 has discussed this ambition, it has come with little detail on financing that would change market dynamics for internet infrastructure – particularly in Africa. Alongside a funding offer, DIDA should advocate for competitive markets around the world and help their cutting-edge firms to expand fairly and responsibly in new digital markets, in turn providing the platforms and services upon which businesses, both physical and digital, can build their own futures.

In practice, DIDA should coordinate investment in infrastructure and ensure access to close the digital divide by 2030. As TBI analysis has previously set out, the investment necessary to close this gap by 2030 is approximately $450 billion. To put this cost in perspective, raising these funds would require member countries of the Development Assistance Committee – an arm of the Organisation for Economic Cooperation and Development (OECD) – to contribute just 0.02 per cent of their gross national income (GNI) per year. This is a small price to pay for a foundational investment that would enable low- and middle-income countries to forge their own paths to prosperity and expand the global internet economy to everyone’s benefit.

Members of DIDA should also develop a programme of expanded trading relationships and investment opportunities in the broader internet ecosystem, particularly elements that boost demand for internet services in emerging economies. On the technology side, this means policy to incentivise investment in servers and core infrastructure that make the internet more reliable, as well as investment in software (for example, payment and cybersecurity systems) because modern infrastructure will help facilitate advanced economies. It should also mean facilitating trade in cultural goods – supporting the cultural and social vibrancy of online communities can help grow digital economies from the ground up. Investing in creative sectors in 2021 has never been more cost-effective with modern digital tools and platforms such as YouTube and TikTok. There are positive externalities of greater consumption of digital cultural goods such as the build-out of content delivery networks (CDNs) that can offer entertainment, education or e-commerce services. The aim should be for the internet giants’ network of CDNs around the world to look more like it does in North America and in Europe.

2. Strategic Geopolitical Status: A New Settlement With Global Tech

The geopolitical power of many tech companies is now a fact: hyperscale technology players operating globally, in multiple adjacent sectors, often control several vertical layers of the internet stack. From submarine cabling to smartphone apps, these firms have an outsized role in shaping the internet as one of the world's most important economic and social infrastructures.

So far, the geopolitical importance of some technology companies has primarily been acknowledged via ad hoc investigations into foreign takeovers (for example, NVIDIA/ARM or Nexperia/Newport Wafer Fab in the UK) or national security (in the case of TikTok in the US, or global bans on Huawei components in 5G networks). While merited, this is a very narrow view of internet geopolitics and these decisions are highly reactive, focused only on combatting the domestic spread of foreign (mostly Chinese) tech players. There is comparatively little attention given to the proactive role that US, UK and EU tech companies – and any others that have benefitted from a liberal, open internet model – could play to protect, preserve and promote this model internationally.

A new approach should start with the UN designating a new class of firms with "strategic geopolitical status" to formally recognise the global importance of some of them. This approach builds on competition proposals in countries like the UK, which plan to treat "strategic market status" firms as a special class with corresponding rights and responsibilities. In practice, this approach should include three critical mechanisms:

1. Requirement to establish and/or join a **geo-technology board,** a new type of independent, industry-wide, self-regulatory body for global technology companies with significant geopolitical importance
2. These new bodies (and there could be multiple) should have **non-member observer status at the UN** to provide an authoritative touchpoint between global policymakers and technology companies
3. Requirement for firms to set out a new **international policy**, recognising their role as global proponents for a secure, open, liberal internet model

Defining the precise threshold for this equivalent "strategic geopolitical status" designation is beyond the scope of this report, but taking a global view and considering firms that operate in more than 50 countries, have more than 50 million monthly active users (for consumer tech companies), and have annual revenues of more than $1 billion and/or a market capitalisation or private valuation of more than $30 billion would be a good place to start before working down to smaller companies with outsized impact (such as Reddit).

A. Geo-Technology Boards: A New Regulatory Model

There are several domains where technology companies are playing a more active, global role. On content policy, social-media players act as a "frontline enforcer" based on varied national rules while also taking extraordinary, and sometimes divergent or inconsistent, decisions to moderate the actions of some world leaders on their platforms. Large services also act as de facto elements of the state apparatus, delivering contracts for governments and militaries, or working closely with law enforcement and intelligence agencies on countering terrorist and child abuse content, as well as cybercrime attribution and other national-security risks. Companies including Facebook and Google also provide basic internet services and submarine data cables to underserved communities around the world.

These geopolitical issues are not reducible to any one narrow policy area or domestic regulator. That makes regulation by individual states insufficient and prone to divergence. On the other hand, while critics of the tech industry bemoan the apparent failure of self-regulation, this is misplaced. The status quo of voluntary, individual and uncoordinated decision-making is an entirely different model from proper, enforced self-regulation with mandatory codes of practice and industry-wide enforcement. The latter looks more like the US Bar Association or the UK's Advertising Standards Authority than merely a "lawless wild west".

Facebook's Oversight Board has shown the benefits of creating an independent governance mechanism and challenge function, but its impact is limited to one company and its scope is focused only on content decisions. In contrast, a broader self-regulatory body open not just to the largest tech firms or most visible social-media companies but also to infrastructure services like Cloudflare and Stripe could offer more effective, industry-wide accountability on important geopolitical issues.

An industry self-regulator could have numerous benefits for tech companies across arenas, creating opportunities for more unified and coherent engagement. Better coordination of policies could reduce liabilities; smaller companies can benefit from pooled policy capability and resource; and making this model work could also avoid a costly, misplaced alternative of utility-style regulation from yesteryear. The technology industry does already collaborate on some issues, such as cybersecurity or terrorist and child sexual abuse material (CSAM), but a formal body providing a more consistent engagement route for nation-states would be a step forward.

B. Observer Status at the UN

Nongovernmental organisations have been able to participate in some form in UN deliberations since its inception. Organisations have participated in the Economic and Social Council (ECOSOC) since 1946 in a consultative capacity, with 5,593 currently having active consultative status. This type of status is limited, however, as it is dependent upon invitations to individual meetings.

The UN itself may grant non-member states, international organisations and other entities the status of Permanent Observer. The criteria for granting this status have no set basis in the UN Charter or the General Assembly Rules of Procedure and the status can be conferred on states and intergovernmental organisations "whose activities cover matters of interest to the Assembly." Observer status allows the organisation to have access to UN fora, other than the Security Council, but the organisation **cannot propose resolutions** and also **cannot vote** on proposals and resolutions. Observer organisations do not all maintain permanent missions at UN headquarters.

A wide range of organisations have been granted observer status, including the International Chamber of Commerce (ICC) in 2016 on the basis of "its special role and authority as a representative of the business community in more than 120 countries." This also met the need that the UN had identified to give greater opportunities to the business community "to contribute to the realisation of the goals and programmes of the organisation." Advocates for the ICC's accession emphasised the lack of representation of the business sector and the need for greater participation of the private sector in achieving the 2030 Sustainable Development Agenda.

For nation-states, extending this principle of representation to a technology industry that is increasingly important geopolitically has several benefits. Just as the ICC was granted observer status in recognition of the private sector's role in achieving sustainable development goals (SDGs), the activities and decisions of private tech companies are increasingly important for achieving global public goals in health (SDG 3), education (SDG 4), economic growth (SDG 8) and innovation (SDG 9).

UN representation would also provide a critical touchpoint between firms and policymakers so that company decisions with wider geopolitical impact weren't made in a vacuum. Social-media bans on world leaders, for example, should remain the prerogative of private services, but engagement at the UN could allow a wider, more accountable discussion of the frameworks behind these decisions, or highlight inconsistent application of rules.

For smaller countries, a permanent representation at the UN for the global tech industry would also be a way of engaging companies in lieu of creating a new tech ambassador and staffing a new diplomatic corps, as many wealthier countries have been able to do. In this way, UN representation could be more equitable, particularly for the LMICs that will come to shape the future of the internet in global technology governance.

For industry, being represented at the UN would weaken the criticism that tech executives take global decisions without accountability, while giving companies the opportunity to advocate for coherent, liberal, globally aligned internet policies. Many of the most geopolitically important companies have been built in a liberal regulatory model and value system, and this is reflected in their missions. For example, Facebook's stated mission is to "give people the power to share and make the world more open and connected", while Google's is "to organise the world's information and make it universally accessible and useful". When meaningful internet access is increasingly under threat, and global internet regulations are increasingly diverging, technology companies have both a moral and economic incentive to promote a liberal, interoperable model globally. Effective engagement at the UN could promote this.

C. International Policies of Tech Firms

Recognising their role as beneficiaries and proponents of a secure, open, liberal internet model, firms with Strategic Geopolitical Status should be required to set out a new international policy. At minimum, this should include:

- Coordination on world-leader social-media policies to ensure consistency
- Investment in local language-moderation capabilities to minimise social unrest globally and weaken the incentive for countries to block website access
- Establishment of a framework to review the activities of firms in authoritarian states in order to uphold liberal values and avoid being complicit in repression
- Participation in efforts to limit and attribute cybercrime
- Cooperation with a new Multi-Stakeholder Panel on Internet Policy, modelled on the expert IPCC in climate policy, to share data on the health of global online networks and anticipate future risks

3. Oversight from a Multi-Stakeholder Panel on Internet Policy (MPIP)

While DIDA would represent a mechanism for nations to cooperate on internet governance, there remains a wider class of issues where global action is necessary. In particular, in order for actors to fully engage in the diplomacy required for internet internationalism, they require the knowledge, support and objective criteria of the impacts of potential changes on the entire ecosystem. Technical discussions about the internet remain too disconnected from political debate, with decisions often focused on short-term priorities at the expense of long-term issues. Similarly, consensus on the need for reforms means little if there is nobody to hold the key geopolitical actors accountable on delivering those changes.

Reforms to multi-stakeholder fora and UN bodies remain challenging. While there is widespread consensus about the need for improvements, there is little agreement about the specifics, and debates over restructuring have become battlegrounds between states, companies, technical experts and civil society, making meaningful change impossible. Crucially, there is no independent body helping to negotiate an agenda or acting as an early-warning system if there is erosion of the internet ecosystem.

A promising model is the Intergovernmental Panel on Climate Change, the UN body that has an important function in global climate action, distilling the scientific into the political and ensuring that leaders can take action. There is a gap in the internet ecosystem for a parallel organisation, as recommended by the UK–China Global Issues Dialogue Centre at Jesus College, University of Cambridge. An expert-led, multi-stakeholder oversight body could provide a form of "semi-formal" diplomacy to plug this gap by properly equipping global leaders. It should sit outside of both existing multi-stakeholder fora and UN bodies, avoiding their challenges, without replacing their undoubted merits or triggering broader debates about reform that sap all available time, energy and resource.

The MPIP should be charged with providing the knowledge and insights to enable the protection of the internet ecosystem, including proposals for the renewal of existing institutions. This should include improved spaces to evaluate the policy impact of technical proposals and far better representation of the global internet community, particularly LMICs. If such reforms do not happen, these organisations risk declining in relevance even further – at least in the mindset of some key industry and geopolitical players. In this scenario, it may be necessary for the MPIP's remit to expand beyond merely an independent, ecosystem oversight body.

Crucially, membership should not be restricted to nation-states. Robust analysis of the health of both public and private infrastructure and networks would require cooperation with technology companies and telecoms providers. Involving them could, in turn, provide a formal means of recognising their geopolitical power in a way that the Internet Governance Forum has not been able to do. As discussed, the opportunity to be represented at a newly authoritative, global internet forum could also act as an incentive to technology companies to actively cooperate on promoting an open, internationalist internet.

4. Integrated Digital, Data and Tech Foreign Policy

In order to build a coherent approach to engagement in standards and regulatory bodies as a foreign-policy priority, countries should develop an integrated foreign-policy incorporating a technology strategy. This should include empowering a cadre of technology diplomats and ambassadors who are well-equipped to negotiate across various multi-stakeholder and multilateral governance bodies and can build novel coalitions to stabilise the internet ecosystem. This could mean:

- A tech diplomatic corps to liaise with private tech companies through policy pipelines, bilateral tech hubs and clusters globally
- Actively supporting an open and progressive vision of the internet as central to liberal democratic values, and critical to helping emerging economies reap the full economic, social and cultural benefits of the tech revolution
- Coordination with like-minded nations on a consistent and coherent message in international standards-setting bodies for responsible and ethical standards within new technologies
- Alignment between domestic ministries that engage in international fora to ensure the development of international-governance initiatives that support responsible development and use of new and emerging tech such as distributed ledger technology (DLT)
- Broad international cybersecurity cooperation including technical assistance and capacity building that not only reduces the global digital divide, but also supports the growth of emerging digital economies and facilitates the beneficial uses of new and emerging technologies

Conclusion

The internet ecosystem is at a critical tipping point. However, the perception that the challenges it faces are so great they cannot be resolved could condemn it to a future that we must all seek to avoid. Yet current approaches range from outright avoidance to extreme competition on the fundamental protocols on which the internet is built. Both strategies will ultimately lead to the unravelling of the internet as we know it.

The mindset and practical steps of internet internationalism can help tilt the future towards a more progressive, sustainable and globally beneficial internet. This new model provides the framework to step back and visualise areas of common interests, to harness the benefits of mutual cooperation, to maximise the value in stepping away from polarised narratives and to build an objective knowledge base for effective decision-making. It will provide the guidance for leaders to develop national, regional and international capacity to align and engage with critical stakeholders in order to preserve and enhance the global, open and interoperable internet – which underpins immense social and economic prosperity for all.

Acknowledgements

The authors are extremely grateful to the following for sharing their expertise as part of the research behind this report:

- **Adeboye Adegoke**, Senior Program Manager, Paradigm Initiative
- **Karoliina Ainge**, Cybersecurity and Technology Lead, Independent Diplomat
- **Kevin Allison**, Director, Geo-technology, Eurasia Group
- **Felicia Anthonio**, Campaign Coordinator, Access Now
- **Katja Bego**, Principal Researcher and Future Internet Lead, Nesta
- **Jochai Ben-Avie**, Steering Committee Co-Chair, Connect Humanity and Fellow, Atlantic Council
- **Lily Edinam Botsyoe**, Community Engagement Lead, Hacklab Foundation
- **Chris Cash**, Researcher, China Research Group
- **James Crabtree**, Executive Director, Asia, International Institute for Strategic Studies
- **Tanya Filer**, Founder, StateUp and Policy & Research Leader, Bennett Institute, University of Cambridge
- **Ben Greenstone**, Managing Director, Taso Advisory
- **Linda Griffin**, VP, Global Public Policy, Kry / Livi
- **Dom Hallas**, Executive Director, Coadec
- **Rose Jackson**, Director of the Policy Initiative, Atlantic Council Digital Forensic Research Lab
- **Dr Konstantinos Komaitis**, Policy Fellow, Brave New Software Foundation
- **Sébastien Krier**, Senior Technology Policy Researcher, Stanford Cyber Policy Center
- **Dominique Lazanski**, Director, Last Press Label
- **Kieren McCarthy,** Executive Director, IFFOR
- **Nick Merrill**, Director, Daylight Lab, UC Berkeley Center for Long-Term Cybersecurity
- **Julia Pamilih**, Researcher, China Research Group
- **Andrew Roughan**, Managing Director, PLEXAL
- **Emily Taylor**, CEO, Oxford Information Labs and Associate Fellow, Chatham House
- **Antoine Vergne**, Co-Director, Missions Publiques
- **Chris Worman**, VP, Alliances and Program Development, TechSoup and Steering Committee Co-Chair, Connect Humanity

Charts created with Highcharts unless otherwise credited.

FOLLOW US

facebook.com/instituteglobal
twitter.com/instituteGC
instagram.com/institutegc

GENERAL ENQUIRIES

info@institute.global

FIND OUT MORE
INSTITUTE.GLOBAL