John Barrow famously declared the independence of cyberspace in 1996 – describing it as a unique space in which governments were not welcome and would be allowed no control. (Reflecting the Zeitgeist, Barrow was both an internet civil liberties pioneer and a lyricist for psychedelic rock band the Grateful Dead.)

‘Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of the Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.’

Seen as naïve even at the time, what has since emerged is a structure of internet governance designed to address a range of societal and policy issues. At my organisation, Diplo, we describe this as a building with seven floors, or levels. (See illustration, page 15.)

It begins with infrastructure, including standards and security – once a firm ground which is now becoming shakier. The legal level encompasses jurisdiction issues, intellectual property rights, copyright, labour law and other aspects of law. Development, especially important for small and developing countries, includes knowledge transfer, boosting development in markets, and innovation. The economic level includes taxation, e-commerce, the gig economy and markets broadly. Increasingly, many of these issues are being discussed under the framing of free flow of data. We describe as ‘sociocultural’ issues of multiculturalism, education and diversity, with human rights covering privacy and freedoms, among others. It is interesting to observe the number of people or idea groups that are working on this construction, from IT professionals and engineers to governments, multinational corporations, human rights movements and grassroot user organisations, to international organisations (all mixed in a big soup of acronyms) – this is the multi-stakeholder environment that is shaping the internet today.

THE GEOPOLITICAL INTERNET

The digital world is increasingly being driven by ideology rather than efficiency, with profound impacts on governance and the digitalised society, argues VLADIMIR RADUNOVIC. Political trends are shaping the regulatory environment, and regulators need to adapt.
Digital Sovereignty and Interdependence

25 years after the Barrow declaration, this structure reflects 'an age of interdependence', in which the UN has called for co-operation in areas such as an inclusive digital economy, human rights, trust and security, and institutional capacity. Interconnectivity means that the same standards are being pursued globally, with the internet maintained as a single space. Yet, the concept of 'digital sovereignty' is growing in prominence. Russia and China are very open about their demands for sovereignty and are setting up national firewalls, and the EU asserts its right to act independently in the digital world, with its own cloud and even a DNS resolution system. The US has introduced protective economic and regulatory measures against the influence of China, attempting to rely only on the digital supply chain from like-minded states – and its own. Many small and developing countries treat the localisation of national data as a policy priority partly in response to the enormous power that foreign big tech has accumulated. Whether good or bad, this will result in a fragmentation of the 'digital axis'.

For example in routing, priority may be given to ideology over functionality – to whether data is going through an unfriendly territory rather than by the quickest global route. This is changing international standards and the implementation of core internet protocols, including DNS and BGP (border gateway protocol), increasing fears among internet communities about the 'splinternet' – a fragmentation of the global internet into parts that are less interoperable or even disconnected one from another.

In response, governments are increasing their regulatory grip. The EU has brought in a number of regulatory acts, such as the Digital Services Act, the Digital Markets Act and the General Data Protection Regulation, which shape not only the political environment of Europe but also impact how other countries treat the localisation of national data as a policy priority partly in response to the enormous power that foreign big tech has accumulated. Whether good or bad, this will result in a fragmentation of the 'digital axis'.

Another point we can note is that a range of actors – telecoms, content, infrastructure – are mixed across different levels. Digital convergence is resulting not only in telecoms companies offering or creating content as part of their packages, but also cloud and service providers (Google, Meta or Microsoft) operating at the telecommunications level, for example by laying cross-continental submarine internet cables. Business models based on vast data collection often enable existing monopolists to lead in other areas, like AI. Convergence creates complexities in many areas, from DNS protocols and cybercrime to content issues such as hate speech and disinformation. It also influences policies around emerging technologies like the metaverse which connects VR and AR solutions, social media platforms, and crypto and blockchain technologies. Traditionally governments have turned to telecoms regulators to deal with these issues. But these bodies may not have a sufficient understanding of the internet or the content issues, especially while definitions of those concepts continue to change.

Connectivity

Cables are a critical part of the connectivity of smaller countries and there have been many improvements in recent years, especially in Africa and the Caribbean. But this too is geopolitical, shaped by the flow of the data and the ability to access information. Many cable networks are created by public-private partnerships, or by big players like Meta and Google. This raises the question of what ownership a small country has – for example, who is liable if a cable is broken, especially where it’s crossing a continent. This concern is inflated in times of increased threats of military operations against submarine cables, as a result of geopolitical tensions and hybrid (or open) warfare. The emerging issue is that of satellites, with some countries launching their own, and some commercial satellites operating semi-independently from governments while having great national importance, as witnessed in the case of Starlink following a tsunami in Tonga or for reconnecting Ukraine during the war with Russia. Other regulatory questions emerge in relation to satellite connection provided by global big tech: how does a country exert control and how does it manage issues such as spectrum and conditions for connectivity.

Cross-border data flows

Source: UNCTAD
Another aspect of connectivity is the value of the data flow. There is a natural discrepancy between larger and smaller countries, in part a bandwidth issue, but also because the global companies providing services store their customer data in the cloud, mainly in developed countries. This has a profound effect on the distribution of power. Whoever collects the data can then sell it, and many big tech companies have a turnover comparable to the GDP of a developing country. This provides large technology companies with the influence to shape many policy issues, including competition, taxation (and its distribution), privacy and content policy, and what happens to citizens’ data. Should Google be the organisation to use data for the development of AI and then monetise it? Is there an opportunity for small and developing countries instead? And can this be done by regulation or by creating the environment where this is possible? This is another area where smaller states could work together in a coalition to better negotiate with big tech to set favourable conditions thanks to their bigger market and political power when working together.

**CONTENT AND CYBERSECURITY**

The world hasn’t had to deal with politics and negotiations around content much in the last few decades but now there are huge challenges for social media policies to address issues of disinformation, hate, cybercrime and the dark web without crossing the lines of human rights, free speech and broader freedoms. It’s hard to balance these at a national level. Harder still when taking into account global relations.

Arguably, there is no such thing as ‘cyberspace’ or an ‘offline life’. Everything is connected, and everything can be hacked. Increasingly the targets are critical sectors of society, such as energy and healthcare. Costa Rica was locked down for months in a ransomware attack that was supposedly criminal. The threat has evolved from kids and hackers, to criminal gangs, sometimes tolerated and sometimes enabled by states. Countries are openly developing offensive cyber capabilities, many with unlimited resources and political will. So high politics – what’s happening in Ukraine and between China and the US, for instance – is something that businesses and governments need to take account of in their threat modelling.
THE BATTLE FOR THE ITU
Politics is also influencing the adoption of standards. There are battles over, for example, whether human rights should be embedded in new internet protocols, or whether they should include more sovereignty and control. These issues reached the governance of the International Telecommunication Union, which for years hadn’t been seen as especially important for geopolitics. The body responsible for creating standards and interoperability had seen increasing political influence, particularly from Russia and China. Their vision for the internet, focused on rejecting ‘American dominance’, was represented by the Russian candidate for secretary general in the recent leadership election, Rashid Ismailov. At the 2022 Plenipotentiary Conference in Bucharest, however, it was the US candidate, Doreen Bogdan-Martin, who was elected as the new secretary general.

Emerging technologies mean that policies need to be future-proof, and there is much buzz around new concepts like the metaverse. The best way to look at this is to consider the building blocks – in this case blockchain, AI, augmented reality, quantum computing – and examine the challenges and policies related to them. What are the building blocks that can’t be seen, and what impact will they have when put together in the metaverse? The buzz can often lead to disillusionment, so it’s important to be wary of ‘overhype’.

REGULATORY APPROACHES
The roll-out of a technology like 5G raises multiple issues, including infrastructure security, content and protocols, which in turn require a multi-disciplinary approach. This is a particular capacity challenge for smaller countries without access to the range and depth of skills available to larger jurisdictions. However, at Diplo we see many individuals from small states, with specialist knowledge, who are involved and recognised in global internet governance processes. They are often not consulted by their governments, because they are actors from business or NGOs, or the tech community, but they represent a valuable resource. These people could be mapped, perhaps by cyber ambassadors or line ministries or regulators, and utilised to supplement capacity.

CONTENT REGULATION
Content regulation is always at risk of extending into internet regulation and then censorship. There is a difference between regulating traditional broadcasters and new media with a different modality but which in many cases operate like broadcasters, for example in the streaming of live video. Often these are viewed at larger scale and as quickly as traditional broadcasters. The massacre in Christchurch, New Zealand in 2019 was live-streamed and re-broadcast many times on social media – content which most believe should have been censored outright. But there is a thin line between content regulation and internet censorship. Because so much content is broadcast in jurisdictions over which a regulator may have no control, there is certainly a need for better cross-border cooperation. While there is a distinction between curated and non-curated content, a company like Netflix operates much more like a broadcaster than, for example, Facebook. Pushing on these ‘new media’ companies too hard will result in them self-censoring and valuable content could be lost. An open policy challenge is how to distribute responsibility, set clear criteria about objectionable content and enhance capacities for policing such content, including the proper and ethical use of AI to assist humans.

CRYPTO AND NFTS
NFTs and cryptocurrencies raise particular issues for all economies, but especially for small jurisdictions. Here the use of policy rather than regulation is likely to be most productive, working with developers or the crypto community. It’s important to avoid overhype but also to avoid responding to overhype with overregulation. While primarily the responsibility of financial regulators, NFTs incorporate issues of creativity and copyright, or smart contracts, and so require broad regulatory involvement.

SUMMARY
Geopolitics leans heavily on the digital environment, shifting the internet increasingly away from the functional and towards the ideological. Cyberspace has blended with the real world without recognising real world borders. As everything is cross-border, so must be co-operation and above all diplomacy. The ‘three Ms’ of internet governance are multi-disciplinary, multi-stakeholder, and multi-level. It’s a holistic area that needs all hands to work and cooperate at the local, regional and national level. Governance is a diversified portfolio, not the responsibility of a single ministry, because everything in the political environment, from energy and finance to education, has a digital component. Internet governance needs to be approached holistically – through a ‘whole of government’ and ‘whole of society’ approach.