

## Summary of the discussion

### Introduction

1. **The IGF Policy Network on Internet Fragmentation (PNIF)** was set up to address the question of Internet Fragmentation, to raise awareness of actions and measures that risk fragmenting the Internet, and to facilitate discussion on what could be done to avoid fragmentation. To support a holistic dialogue on fragmentation, the PNIF developed its [PNIF Framework for discussing fragmentation](#) that differentiates between fragmentation of the Internet *User experience*, fragmentation of Internet *Governance and coordination*, fragmentation of the Internet's *Technical Layer*, and technical, political and commercial developments that may have an impact on fragmentation.
2. **The PNIF main session at the IGF 2025** in Norway ([summary](#)) reiterated that UN Member States committed to promoting international stakeholder cooperation to prevent, identify and address risks of Internet fragmentation ([GDC, art. 29, c](#)) and identified the following trends that may cause or worsen Internet fragmentation in 2025:
  - Digital sovereignty and re-territorialisation are used to strengthen state power for national and economic security and protectionism amid rising geopolitical tensions.
  - Normalisation of Internet shutdowns, censorship, network fragmentation as instruments of governments.
  - Persisting gaps in stakeholder insight in the technical coordination of the Internet.

The session concluded that the PNIF is well positioned to develop recommendations on GDC implementation concerning Internet fragmentation.

### Opening statements

3. Christian Dawson, Executive Director of the Internet Infrastructure Coalition (i2Coalition), warned that policymakers often don't accept the arguments about problems with Internet fragmentation. Based on regular contacts with legislators, he observed that these arguments are difficult to understand, especially because they usually focus on jurisdictional issues. Therefore it is necessary to shift the focus when talking to legislators and regulators, and highlight potential problems due to over-blocking and the operational and compliance

burden imposed on companies. The abstract problem of a fragmented Internet needs to be translated into tangible harms that politicians should care about, such as economic and trade impacts, or security risks. In some cases, in particular in a geopolitical context, arguments that a (foreign) government-controlled Internet or DNS undermines human rights can be effective. A recent [DNS at Risk report](#) explains the problems caused by domain and IP blocking through 13 case studies from around the world.

Governments may claim that blocking is the only way to mitigate the harms they are trying to address. To counter this, it is important to redefine the problem, highlight what is already being done within the Internet ecosystem to address it, and point out that takedowns are rarely effective solutions. Most issues can be handled domestically through proper laws and enforcement, while the more complex cross-boarder cases may require strengthening and modernising existing intergovernmental procedures, for example to handle cross-boarder warrants.

4. Alexandre Costa Barbosa, focussed on the governance and sovereignty aspect. He defined digital sovereignty as the capacity of states to conceive, develop and keep digital infrastructure. He highlighted the significant market concentration in data processing infrastructure, which is predominantly in the hands of US based companies. This situation has triggered the emergence of digital sovereignty agendas around the world.

BRIC countries have become a main challenger of the multilateral order, however, with the intention to promote and sustain it. The BRICS civil society defines that digital sovereignty “must be positioned as a multilateral process, integrating public interest and participation, government policy and technical autonomy, while respecting socio-cultural specificities and maintaining equitable access to resources. This includes the promotion of a people-oriented vision of digital sovereignty, based on guaranteeing the autonomy and integration of the people of the BRICS countries.”

Digital sovereignty is understood in the above definition as a self-determination, taking into account territorial, cultural and historical specificities. It includes cybersecurity and information security, education, digital development, and access to emerging technologies and their deployment.

The changing geopolitical order and the shift to a multipolar environment gives rise to new organisations and cooperations such as BRICS. These new organisations, however, do not jeopardise but strengthen what already exists and the UN-based multilateral order.

Avoiding fragmentation in Internet governance means continuing to support the UN-led model in which technical organisations and private actors work together to define the future development of the Internet, while safeguarding the interoperability of internet protocols.

One needs to accept that today's world is different from the world 30 years ago, when the commercial Internet developed, and work toward a re-globalisation that is built on digital sovereignty as a way for states to integrate themselves in the global Internet and gain the benefits from it.

Concluding, Alexandre referred to [research](#) that identifies a fourth dimension of digital sovereignty, next to the three dimensions typically described in the literature (state-led cybersecurity policies, Industrial policies and the development of economic capacities to develop a local soft- and hardware industry, and digital self-determination at the individual level. This fourth dimension are communities and collectives that are also claiming digital sovereignty agendas as a way to raise their voice and be listened to.

### **Acknowledgements**

Thank you to all participants to the meeting and to the panellists-discussant **Mr Christian Dawson**, Executive Director of the Internet Infrastructure Coalition (i2Coalition), and Mr **Alexandre Costa Barbosa**, Researcher. The PNIF is coordinated by **Ms Tereza Horejsova**, MAG member, PNIF co-facilitator, **Ms Sheetal Kumar**, PNIF co-facilitator, **Ms Bruna Martins dos Santos**, PNIF co-facilitator, **Mr Wim Degezelle**, Consultant PNIF, IGF Secretariat.

### *Links*

[PNIF webpage](#)

---