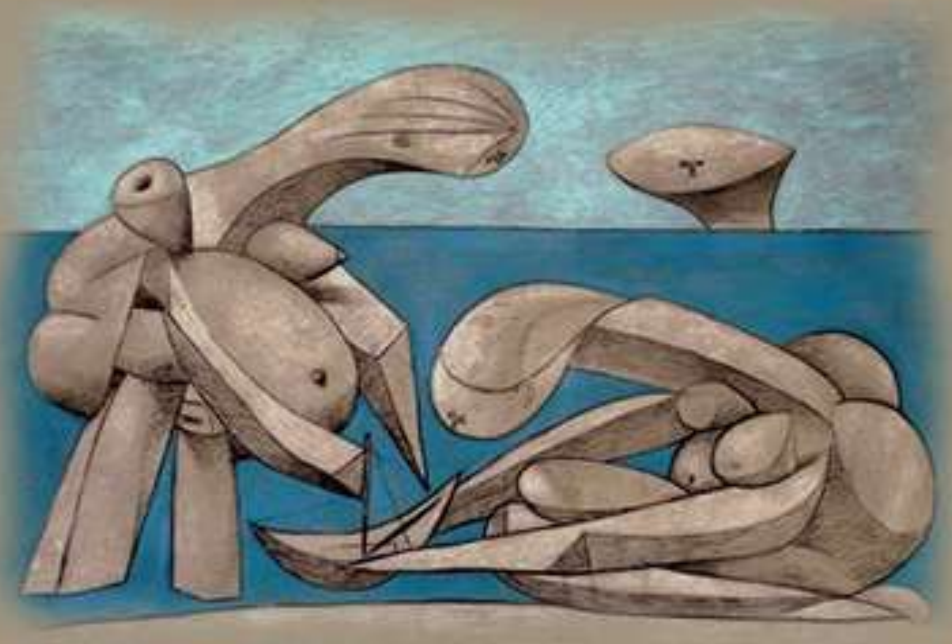
Journal du Droit Transnational



Directeurs:
Ilias Bantekas
Catherine Maia
Tarcisio Gazzini
Francesco Seatzu

www.journaldudroittransnational.it

Vol. 2 – 2026

THE ENVIRONMENTAL FOOTPRINT OF DIGITAL INFRASTRUCTURES: ASSESSING THE REACH AND LIMITS OF INTERNATIONAL ENVIRONMENTAL LAW

Nicolò Andreotti[1]

Abstract
Digital infrastructures are often described in immaterial terms, yet their environmental footprint is substantial and rapidly expanding. Data centres, high-performance computing clusters, and cryptocurrency-mining facilities rely on energy-intensive hardware, water-demanding cooling systems, and globally interconnected electricity grids. These material foundations generate environmental pressures that are increasingly transboundary but remain largely invisible within international legal and policy debates. This article examines how international environmental law (IEL) applies to the environmental impacts of digital infrastructures and assesses whether existing frameworks are equipped to address them. It maps the material dimensions of digitalisation and evaluates the relevance of customary and treaty-based principles - including the no-harm rule, due diligence, environmental impact assessment, cooperation, biodiversity obligations, and climate commitments.

While these principles are conceptually applicable, their practical operation is hindered by structural challenges: the transnational organisation of digital infrastructures, the invisibility of their environmental footprint, and fragmented governance across environmental, digital, energy, and trade regimes. The article argues that IEL provides a valuable normative foundation but requires targeted reforms - including enhanced transparency, cross-border assessments, sector-specific soft-law standards, and greater institutional coordination - to address the environmental consequences of digitalisation effectively.

1. Introduction

Digitalization is often described in immaterial terms, as ‘the cloud’, as frictionless data flows, as virtual infrastructures detached from physical constraints. Yet behind this metaphor lies a vast and rapidly expanding material footprint. Data centres, high-performance computing clusters, and cryptocurrency mining facilities rely on energy-intensive hardware, water-demanding cooling systems, and globally interconnected electricity grids.[2] As digital technologies become increasingly central to economic development, public administration, and global governance, their environmental impacts are no longer peripheral externalities but emerging drivers of resource consumption and greenhouse-gas (GHG) emissions. The environmental

[1] PhD Candidate in International Law, University of Padua, Italy.
[2] See in detail J. Monstadt, K. Saltzman, ‘How Data Centers Have Come to Matter: Governing the Spatial and Environmental Footprint of the “Digital Gateway to Europe”’ (2025) 49 *International Journal of Urban and Regional Research* 757.

consequences of digital infrastructures are therefore neither abstract nor negligible: they are concrete, measurable, and unevenly distributed across jurisdictions.[3]
Despite this growing materiality, the environmental dimension of digitalization remains underdiscussed in international legal debates. Digital infrastructures are typically regulated through the lenses of cybersecurity, data protection, trade, or industrial policy, while their ecological footprint is treated as a technical or domestic regulatory matter.[4] This fragmentation obscures the transboundary nature of digital environmental impacts. Electricity used to power data centres may be generated in another state; water consumed for cooling may exacerbate local scarcity; and energy-intensive activities such as cryptocurrency mining may relocate across borders in response to regulatory arbitrage. These dynamics raise questions that sit squarely within the remit of international environmental law (IEL), yet they are rarely examined systematically through its general principles and obligations.

This article examines how IEL applies to the environmental pressures generated by digital infrastructures. The argument advanced here is twofold. First, it contends that existing principles of IEL - such as the duty to prevent transboundary harm, due diligence, environmental impact assessment, and cooperation - are, in principle, applicable to digital activities. Second, the article argues that the diffuse, cross-border, and often opaque nature of digital infrastructures significantly constrains the effective operation of these principles in practice, particularly at the level of national implementation. Challenges of attribution, monitoring, data availability, and regulatory coordination undermine the capacity of states to discharge their environmental obligations in relation to digital activities. The resulting gap is therefore not primarily normative, but procedural and institutional.

The analysis proceeds in five parts. Section 2 maps the environmental footprint of digital infrastructures, focusing on energy consumption, water use, and cross-border electricity sourcing, with cryptocurrency mining serving as a particularly illustrative case. Section 3 examines the applicability of IEL to these activities, with particular attention to recent developments in international jurisprudence. Section 4 assesses whether existing legal

[3] For the purposes of this article, 'digital infrastructures' refer to the physical systems that enable data storage, processing, and transmission. The ISO/IEC 30134-1:2016 standard defines a data centre as 'a structure, or group of structures, dedicated to the centralized accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control, along with the necessary levels of resilience and security required to provide the desired service availability'. These infrastructures comprise several interdependent layers: network equipment (routers, switches, firewalls) that regulates connectivity; storage systems (hard drives and solid-state drives) that retain ever-growing volumes of data; and computing infrastructure (servers and application delivery controllers) that runs software applications and services.
[4] See e.g., L. Munn, 'Injecting Failure: Data Center Infrastructures and the Imaginaries of Resilience' (2020) 36 *The Information Society* 167; K. Furlong, 'Geographies of Infrastructure II: Concrete, Cloud and Layered (in)visibilities' (2021) 45 *Progress in Human Geography* 190; Y. Au, 'Data Centres on the Moon and other Tales: a Volumetric and Elemental Analysis of the Coloniality of Digital Infrastructures' (2024) 12 *Territory, Politics, Governance* 12.

frameworks are sufficient in practice and identifies the structural limitations that hinder their effectiveness. Section 5 considers potential pathways for strengthening transnational environmental governance in this area. Section 6 concludes by arguing that digital infrastructures must be understood - and regulated - as environmental actors within international law.

2. The Environmental Footprint of Digital Infrastructures

Digital infrastructures are underpinned by extensive physical systems whose environmental impacts are increasingly significant. Data centres, high-performance computing facilities, and cryptocurrency mining operations depend on land-intensive installations, water-based cooling technologies, and large volumes of electricity drawn from regional and transnational grids. Their environmental footprint therefore spans multiple dimensions, including land occupation, resource extraction, water consumption, energy use, and both direct and indirect greenhouse gas (GHG) emissions. This section maps these environmental pressures in turn, providing the empirical foundation for the subsequent legal analysis.

A. Land Use and Spatial Footprint of Digital Infrastructures

Hyperscale data centres require large tracts of land to accommodate server halls, cooling equipment, substations, and security perimeters. While no universally accepted definition exists, IBM suggests that a hyperscale facility typically houses at least 5,000 servers and spans more than 10,000 square feet (approximately 929 m^2).[5] In practice, the largest data centres far exceed this threshold. The Citadel Campus in Reno, Nevada - operated by Switch - covers 7.2 million square feet (approximately 669,000 m^2 or 66.9 hectares), illustrating the scale of land occupation associated with contemporary digital infrastructures.[6] Their siting decisions frequently intersect with land-use planning, agricultural zoning, and local environmental protection rules. In several regions, the clustering of data centres has contributed to the conversion of agricultural or peri-urban land into industrial digital zones, raising concerns about soil sealing, habitat fragmentation, and long-term landscape transformation.[7]

Cryptocurrency mining operations, while sometimes smaller in physical footprint, can generate comparable land-use pressures. Mining facilities often repurpose existing industrial buildings or locate in remote areas with access to low-cost electricity, such as hydropower-rich valleys or regions with surplus energy capacity. In some jurisdictions, the expansion of mining activities has been accompanied by the construction of new

[5] J. H. Santana Stacciarini, R. Junior de Assis Fernandes Gonçalves, *Data Centers, Critical Minerals, Energy, and Geopolitics: The Foundations of Artificial Intelligence* (2025) SocArXiv, available at https://www.researchgate.net/publication/389376214_Data_Centers_Critical_Minerals_Energy_and_Geopolitics_The_Foundations_of_Artificial_Intelligence, at 5.

[6] SWITCH, *Design, Construction and Operation of Data Centers* (2024) available at https://www.switch.com/locations/.

[7] See e.g., ESOFT Lifelong Learning, *Ireland's Data Centre Expansion: Balancing Growth and Sustainability*, 28 July 2024, available at https://esoftskills.ie/irelands-data-centre-expansion-balancing-growth-and-sustainability/.

energy infrastructures - including substations, transformers, and dedicated transmission lines - thereby extending the spatial footprint of digital activities beyond the mining sites themselves.[8]

Land-use impacts are further amplified by the integration of digital infrastructures into global supply chains. The construction of data centre buildings, cooling systems, and server hardware requires large quantities of steel, concrete, plastics, and critical minerals. The digital economy depends heavily on metals such as copper, lithium, cobalt, palladium, and rare earth elements, which are extracted through environmentally intensive processes and are highly geographically concentrated.[9] The Democratic Republic of the Congo (DRC) accounts for roughly 73% of global cobalt production, while China refines approximately 74% of the world's cobalt and processes around 90% of rare earth elements.[10] These concentrations raise concerns related to deforestation, water depletion, land appropriation, and labour conditions in mining regions.[11] Conflicts over water use and Indigenous rights in Latin America's lithium triangle[12], as well as forest loss linked to Indonesia's nickel boom, illustrate the broader environmental consequences associated with digital supply chains.[13]

The material intensity of digital hardware compounds these pressures. Producing complex electronic devices requires between 50 and 350 times the final weight of the product in raw materials.[14] Manufacturing a single laptop mobilizes roughly 600 kg of resources, while an internet router requires around 500 kg.[15]

At the end of their life cycle, digital infrastructures contribute to the world's fastest-growing waste stream: electronic waste.[16] In 2019, global e-waste reached 53.6 million tonnes and is projected to rise to 74.7 million tonnes by 2030. Much of this waste

---

[8] See e.g., B. Bratcher, *Bitcoin Mining: The Unlikely Catalyst For Cheaper Energy In Texas*, Forbes, 2 November 2025, available at https://www.forbes.com/sites/beccabratcher/2025/11/02/bitcoin-mining-the-unlikely-catalyst-for-cheaper-energy-in-texas/.

[9] United Nations Environment Programme, *Global Resources Outlook 2024: Bend the Trend – Pathways to a Liveable Planet as Resource Use Spikes* (UNEP, 2024), at 5.

[10] USGS, *Mineral Commodity Summaries* (2024) available at https://pubs.usgs.gov/periodicals/mcs2024/mcs2024.pdf.

[11] Orivium, *We know data centres require energy and water, but what about their critical minerals?*, 29 August 2025, available at https://oriviumglobal.com/we-know-data-centres-require-energy-and-water-but-what-about-their-critical-minerals.

[12] P. Bolados García, S. Babidge, 'Ritualidad y Extractivismo:La Limpia de Canales y las Disputas por el Agua en el Salar de Atacama– Norte de Chile' (2017) 54 *Estudios Atacameños* 201.

[13] See in detail B. Hudayana, X. Suharko, A. B. Widyanta, 'Communal Violence as a Strategy for Negotiation: Community Responses to NickelMining Industry in Central Sulawesi, Indonesia' (2020) 7 *Extractive Industries and Society* 1547.

[14] Ibid.

[15] See generally, United Nations, *Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future* (United Nations Publications, 2024).

[16] J. Roundy, *Assess the Environmental Impact of Data Centers*, TechTarget, 12 July 2023, available at https://www.techtarget.com/searchdatacenter/feature/Assess-the-environmental-impact-of-data-centers.

contains toxic additives and hazardous substances, and in many low- and middle-income countries inadequate recycling infrastructure leads to unsafe disposal practices.[17] Data centres themselves can also become obsolete; abandoned facilities may leave behind contaminated materials, waste, or derelict buildings.[18]

B. Cross-Border Electricity Sourcing and Grid Integration

Digital infrastructures are deeply embedded in regional and transnational energy systems. Data centres routinely draw electricity from interconnected grids that span multiple jurisdictions, making it difficult to attribute environmental impacts to a single state. The scale of electricity demand underscores the significance of these dynamics. In 2023, United States data centres consumed an estimated 176 terawatt-hours (TWh) of electricity, more than the annual consumption of the entire state of New Jersey.[19] They accounted for roughly 4 percent of national electricity demand, a share projected to rise to between 6 and 12 percent by 2028.[20] This surge is a key driver of the anticipated 15 to 20 percent increase in UNITED STATES electricity consumption over the next decade. Similar trends are emerging globally as cloud computing, artificial intelligence, and high-performance computing expand.[21]

Cryptocurrency mining further illustrates the transnational nature of digital electricity use. An average Bitcoin mining unit requires around 1.5 kW of continuous power - roughly equivalent to the daily per-capita electricity consumption in the United States.[22] In 2017, Bitcoin's total energy consumption was estimated at approximately 13 percent of Turkey's national electricity use, exceeding that of many African states.[23] These figures highlight the magnitude of mining-related electricity demand and its potential to strain regional grids.

Cryptocurrency mining operations are also highly mobile. They frequently relocate to jurisdictions offering low-cost electricity, whether from hydropower, coal, or natural gas.[24] Competitive pressures have driven miners to seek locations with abundant and inexpensive energy, including Arctic regions where cooler temperatures reduce cooling

[17] Ibid.

[18] See in detail P. Brodie, J. Velkova, 'Cloud ruins: Ericsson's Vaudreuil-Dorion Data Centre and Infrastructural Abandonment' (2021) 24 *Information, Communication & Society* 869.

[19] Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *State of New Jersey State Energy Risk Profile* (2021) available at https://www.energy.gov/sites/default/files/2021-09/New%20Jersey%20Energy%20Sector%20Risk%20Profile.pdf.

[20] A. Shehabi et al., *2024 United States Data Center Energy Usage Report* (Lawrence Berkeley National Laboratory, 2024), at 6.

[21] Ibid.

[22] S. Chamanara, K. Madan, *The Hidden Environmental Cost of Cryptocurrency: How Bitcoin Mining Impacts Climate, Water and Land* (Unu Inweh, 2023), at 5.

[23] On the topic, see Ş. Dilek, Y. Furuncu, Bitcoin Mining and its Environmental Effects (2019) 33 *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi* 91.

[24] N. Scott, M. W. Gehring, *Op-Ed: 'Artificial Intelligence's Dual Role in EU Environmental Law: Both a Target of and a Tool for Enforcement?'*, EU Law Live, February 12, 2026, available at https://eulawlive.com/op-ed-artificial-intelligences-dual-role-in-eu-environmental-law-both-a-target-of-and-a-tool-for-enforcement/.

costs. The Swedish company KnCminer, for example, attempted to capitalize on local hydropower and natural cooling before declaring bankruptcy in 2016.[25] In 2019, an estimated 58 percent of global Bitcoin mining occurred in China, followed by the United States with 16 percent. China's dominance was largely attributable to cheap electricity, with many mining centres relying heavily on coal-fired power.[26]

Even seemingly small digital interactions reflect this broader trend. A single ChatGPT query is estimated to consume around 2.9 watt-hours of electricity - nearly ten times more than a traditional Google search (0.3 Wh).[27] While individually modest, such interactions scale rapidly across billions of daily queries, further embedding digital infrastructures within global energy systems.

C. Water Use, Cooling Systems, and Local Environmental Stress

In addition to land and electricity, digital infrastructures require substantial volumes of water, primarily for cooling. Hyperscale data centres rely on water-based cooling systems to maintain optimal operating temperatures, particularly in regions where ambient conditions make air cooling insufficient. In many facilities, cooling accounts for more than 40 percent of total electricity consumption.[28] Water is used through two main technologies: evaporative cooling, which consumes water that cannot be recovered, and non-evaporative cooling, which uses less water but requires more electricity. Beyond direct consumption, data centres also rely on water indirectly through the electricity they draw from thermoelectric and hydropower sources.[29]

The scale of water use is striking. One major AI company reported consuming more than 20 billion litres of water per year for server cooling and on-site electricity generation.[30] Such demand places significant pressure on local water resources, especially in regions already experiencing scarcity or seasonal droughts. According to Bloomberg, nearly two-thirds of new UNITED STATES data centres built since 2022 are located in areas classified as high water-stress zones.[31]

Cryptocurrency mining exhibits similar dynamics. The water footprint of Bitcoin mining alone amounted to approximately 1.65 cubic kilometres between 2020 and 2021 - the equivalent of more than 660,000 Olympic-sized swimming pools, or enough water to

[25] S. Chamanara, K. Madan, *supra* note 22, at 12.
[26] J. Young, New Report Shows China Dominates Bitcoin Mining, Is This a Sign of Worry?, Forbes, 12 December 2019, available at https://www.forbes.com/sites/youngjoseph/2019/12/12/new-report-shows-china-dominates-bitcoin-mining-is-this-a-sign-of-worry/.
[27] EPRI, *Powering Intelligence Analyzing Artificial Intelligence and Data Center Energy Consumption*, May 2024, available at https://www.epri.com/research/products/3002028905, at 4.
[28] P. Li et al., 'Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models' (2025) 68 *Communications of the ACM* 54.
[29] Ibid.
[30] Chamanara, Madan, *supra* note 22, at 6.
[31] L. Nicoletti, M. Ma, D. Bass, *AI is Draining Water from Areas that Need it Most*, Bloomberg, 8 May 2025, available at https://www.bloomberg.com/graphics/2025-ai-impacts-data-centers-water data/.

meet the basic needs of over 300 million people in rural sub-Saharan Africa.[32] Mining facilities increasingly adopt immersion or liquid-cooling technologies to improve hardware efficiency, which also entails water use and, in some cases, thermal discharge into local ecosystems. Although the scale varies across operations, the underlying pattern is consistent: digital infrastructures convert water into a cooling resource, often without transparent reporting or environmental assessment.[33]

The environmental impacts of this water consumption are highly localized. They may include reduced availability for agricultural or domestic use, heightened competition during peak demand periods, and thermal pollution from discharged water. One major AI company disclosed that nearly 80 percent of the water used for on-site cooling was potable, intensifying pressure on municipal supplies.[34]

D. Direct and Indirect Greenhouse Gas Emissions

Although much of the climate impact of digital infrastructures arises through electricity generation, these systems also produce emissions that contribute to global warming. Data centres rely on backup diesel generators to ensure uninterrupted operation during grid instability or maintenance. These generators, while used intermittently, emit nitrogen oxides, particulate matter, and carbon dioxide, and their cumulative impact becomes significant in regions hosting dense clusters of facilities.[35] While some hyperscale operators, like Amazon and Microsoft, have committed to renewable energy and carbon neutrality, many smaller facilities lack the capital to pursue similar strategies.[36]

Cryptocurrency mining operations in particular generate direct emissions, especially when co-located with fossil-fuel-based energy sources. The Bitcoin network relies heavily on fossil energy, with coal constituting an estimated 45 percent of its energy mix.[37] Between 2020 and 2021, Bitcoin mining produced more than 85.89 million metric tons of CO_2-equivalent, comparable to burning 84 billion pounds of coal, operating 190 natural-gas-fired power plants, or landfilling over 25 million tons of waste.[38] In some cases, mining companies have entered into agreements to revive or sustain coal or gas-fired power plants, effectively extending the operational life of carbon-intensive infrastructure.[39]

---

[32] Chamanara, Madan, *supra* note 22, at 6.
[33] Ibid.
[34] Google, 2024 Environmental Report (2024) available at https://sustainability.google/reports/google 2024-environmental-report/.
[35] State of Washington Department of Ecology, available at https://ecology.wa.gov/air-climate/air-quality/data-centers.
[36] S. Gonzalez Monserrate, *The Cloud Is Material: On the Environmental Impacts of Computation and Data Storage*, MIT Case Studies in Social and Ethical Responsibilities of Computing, 27 January 2022, available at https://mit-serc.pubpub.org/pub/the-cloud-is-material/release/2.
[37] Chamanara, Madan, *supra* note 22, at 6.
[38] Ibid.
[39] A. Asher-Schapiro, *Insight-Coal to crypto: The gold rush bringing bitcoin miners to Kentucky*, Reuters, 21 March 2022, available at https://www.reuters.com/article/markets/oil/insight-coal-to-crypto-the-gold-rush-bringing-bitcoin-miners-to-kentucky-idUSL5N2VO4WT/.

In addition to global climate impacts, the expansion of data centre zones has raised concerns regarding local air quality and cumulative emissions associated with emergency power systems. Communities have reported noise pollution from cooling fans and generator testing. During periods of high electricity demand, backup generators may be activated to reduce grid load, releasing substantial quantities of nitrogen oxides and other pollutants that pose respiratory health risks, particularly for vulnerable populations.[40] Taken together, these patterns demonstrate that digital infrastructures generate a combination of direct and indirect GHG, shaped by energy sources, backup power systems, and operational practices. Their climate footprint is thus both geographically diffuse and locally concentrated, reflecting the complex materiality of the digital economy.

3. The Application of International Environmental Law to Digital Activities

Digital infrastructures sit at the intersection of multiple regulatory domains. Trade agreements facilitate cross-border data flows; energy governance regulates electricity markets; digital governance frameworks address cybersecurity, data protection, and platform regulation. Yet these regimes rarely consider the environmental implications of digitalization. IEL, by contrast, is expressly designed to address activities that generate environmental impacts, irrespective of the sector in which they arise.

This section examines how the principles of IEL apply to digital infrastructures, drawing in particular on recent developments in international jurisprudence. While digital infrastructures are not addressed as such in the Advisory Opinion of the ICJ on Climate Change, the Court's interpretation of core environmental obligations provides an important analytical framework for assessing the environmental footprint of digital activities.[41] Against this background, the section identifies both the conceptual coherence of applying IEL to digital infrastructures and the practical challenges that arise when traditional environmental norms confront the materiality and transnational operation of the digital economy. It examines, first, the customary rules of IEL, which continue to play a central role in practice, and, second, relevant treaty-based obligations addressing environmental dimensions of digital activities

A. Customary Rules of International Environmental Law

1. Duty to Prevent Transboundary Environmental Harm

The duty to prevent transboundary environmental harm - commonly referred to as the no-harm rule - requires states to ensure that activities within their jurisdiction or control do not cause significant environmental damage to other states or to areas beyond national jurisdiction. Long recognised as a cornerstone of customary IEL, this obligation has been consistently affirmed in international jurisprudence. In *Trail Smelter*, the arbitral tribunal held that no state has the right to use or permit the use of its territory in a manner that causes serious injury to another state.[42] The International Court of Justice (ICJ)

[40] See e.g., State of Washington Department of Ecology, *supra* note 35.

[41] *Responsibilities of States in respect of Climate Change, Request for Advisory Opinion submitted by the UN General Assembly*, Advisory Opinion of 23 July 2025, General List No. 187 [ICJ Advisory Opinion on Climate Change].

[42] *Decision of 11 March 1941*, United Nations, Reports of International Arbitral Awards, Vol. III, p. 1965.

subsequently reaffirmed this principle in *Corfu Channel*, *Legality of the Threat or Use of Nuclear Weapons*, and *Pulp Mills*, emphasising that states must use all means at their disposal to prevent significant transboundary harm.[43]

Recent jurisprudence has clarified that this obligation applies fully to GHG emissions. In its Advisory Opinion on Climate Change, the ICJ confirmed that climate change results from cumulative emissions and that the no-harm rule therefore applies even where harm cannot be traced to a single source.[44] States must assess and address the combined effects of activities under their jurisdiction and adopt mitigation and adaptation measures capable of preventing foreseeable harm to the climate system and other components of the environment.[45]

The no-harm rule is operationalised through the obligation of due diligence. Due diligence constitutes a standard of conduct that evolves over time and varies according to circumstances.[46] As the Court observed in *Gabčíkovo–Nagymaros*, the required level of diligence increases as scientific knowledge advances.[47] Where there is widely recognised scientific evidence of a high risk of significant environmental harm, states are expected to adopt more stringent preventive measures.[48] Reports of the Intergovernmental Panel on Climate Change (IPCC) therefore play a central role in informing the content of due diligence obligations.[49] At the same time, the Court has acknowledged that due diligence must be interpreted in light of states' respective capabilities, reflecting the principle of common but differentiated responsibilities and respective capabilities (CBDRRC).[50]

As demonstrated in Section 2, digital infrastructures generate environmental pressures - including GHG emissions, water depletion, and land-use change - that may produce effects beyond national borders. These characteristics bring digital activities within the scope of the no-harm rule, which applies to any activity capable of causing significant transboundary environmental harm, irrespective of its technological or economic character.

2. Duty to Conduct Environmental Impact Assessments

The obligation to prevent transboundary environmental harm entails not only substantive regulation but also procedural safeguards designed to identify and address

---

[43] *Corfu Channel case*, Judgment, I.C.J. Reports 1949, p. 22; *Legality of the Threat and Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996 (I), p. 242, para. 29; *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, I.C.J. Reports 2010 (I), p. 56, para. 101; *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment, I.C.J. Reports 2015 (II), p. 706, para. 104.
[44] ICJ Advisory Opinion on Climate Change, *supra* note 41, paras. 273, 276.
[45] Ibid para. 279.
[46] Ibid para. 282.
[47] *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, I.C.J. Reports 1997, p. 77, para. 140.
[48] ICJ Advisory Opinion on Climate Change, *supra* note 41, paras. 283-284.
[49] Ibid paras. 74, 77–83 and 277–279.
[50] Ibid para. 290.

environmental risks in advance.[51] Among these procedural duties, the obligation to conduct an environmental impact assessment (EIA) for activities likely to cause significant transboundary harm is firmly established in customary international law.[52] The ICJ has repeatedly affirmed that due diligence requires states to assess environmental risks prior to authorising potentially harmful activities, particularly where those activities involve significant emissions or resource use.[53]

EIAs serve a preventive function by enabling states to evaluate foreseeable environmental effects, including cumulative and indirect impacts, before decisions are taken. In the climate context, the Court has clarified that EIAs must address climate-related risks where relevant, and that failure to take appropriate preventive measures - including through inadequate assessment - may amount to a breach of international obligations.[54] States are therefore required to regulate public and private actors, adopt and enforce environmental legislation, and update regulatory frameworks in light of evolving scientific knowledge.[55] Regulatory inertia in the face of known environmental risks may constitute a failure to exercise due diligence.[56]

The relevant question is thus not whether a legal basis exists for requiring environmental assessment, but whether particular activities are capable of generating significant environmental effects. As shown in Section 2, large-scale digital infrastructures - such as hyperscale data centres and major cryptocurrency mining facilities - may entail substantial electricity consumption, water use, and associated emissions. Where these effects are foreseeable and potentially significant, such activities fall within the category of projects for which an EIA may be required under general international law.

3. Duty to Cooperate and Exchange Information

The customary duty to cooperate obliges states to exchange information, consult in good faith, and coordinate responses to transboundary environmental risks. Rooted in general international law and reflected in Article 1 of the United Nations Charter[57], this duty has been consistently affirmed in environmental instruments and jurisprudence.[58] Principle 24 of the Stockholm Declaration and Principle 7 of the Rio Declaration both emphasise

[51] Ibid para. 295.
[52] *Certain Activities Carried Out by Nicaragua*, *supra* note 43, para. 104; *Pulp Mills*, *supra* note 43, paras. 101–102, 144–146, 204.
[53] ICJ Advisory Opinion on Climate Change, *supra* note 41, para. 280.
[54] Ibid para. 298.
[55] Ibid para. 282.
[56] Ibid para. 295.
[57] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art. 1.
[58] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, I.C.J. Reports 1986, p. 101, para. 191; ICJ Advisory Opinion on Climate Change, *supra* note 41, paras. 214–218 and 260–267; Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly resolution 2625 (XXV) of 24 October 1970.

that environmental protection depends on cooperative action[59], while international courts and tribunals have recognised cooperation as a customary obligation in cases such as *MOX Plant* and the 2024 ITLOS Advisory Opinion on Climate Change.[60]

Cooperation has a pronounced procedural dimension. The ICJ has stressed the importance of technical cooperation and information sharing in addressing complex environmental challenges, particularly climate change, which it has characterised as a common concern of humankind.[61] Effective mitigation and adaptation depend on the availability and exchange of relevant information, as well as on coordination to ensure that measures adopted by one state do not undermine collective efforts or generate new risks of transboundary harm.[62]

Due diligence may also require states to notify and consult with potentially affected states where planned activities pose a risk of significant transboundary environmental harm. This obligation, affirmed in *Certain Activities* and *Construction of a Road*, applies where notification and consultation are necessary to determine appropriate preventive measures.[63] In the climate context, the ICJ has emphasised the importance of cooperation where activities or policy choices affect shared mitigation efforts or the integrity of climate-related data and strategies.[64]

As illustrated in Section 2, digital infrastructures generate environmental pressures - such as electricity-driven emissions, water consumption, and mining-related land impacts - that may extend across borders and involve shared resources. These characteristics place digital activities within the scope of the customary duty to cooperate, which applies whenever the prevention of environmental harm depends on information exchange, consultation, or coordinated action among states.

B. Treaty-Based Environmental Obligations

1. Protection of Biodiversity

International environmental treaties impose binding obligations on states to conserve biodiversity, protect ecosystems, and regulate activities that may adversely affect ecological integrity. Core global instruments - including the Convention on Biological Diversity (CBD), the World Heritage Convention (WHC), and the Ramsar Convention - require states to establish and preserve protected areas, conserve species, and regulate activities that may degrade ecosystems of high ecological value. The WHC obliges states

---

[59] Declaration of the United Nations Conference on the Human Environment, Stockholm, 16 June 1972, UN Doc A/CONF.48/14/Rev.1, Principle 24; Rio Declaration on Environment and Development, Rio de Janeiro, 14 June 1992, UN Doc A/CONF.151/26 (Vol I), Principle 7.

[60] *MOX Plant (Ireland v. United Kingdom)*, Provisional Measures, Order of 3 December 2001, ITLOS Reports 2001, p. 110, para. 82; *Request for an Advisory Opinion Submitted by the Commission of Small Island States on Climate Change and International Law, Advisory Opinion* [ITLOS Opinion on Climate Change], ITLOS Reports 2024, p. 110, para. 296.

[61] ICJ Advisory Opinion on Climate Change, *supra* note 41, para. 285.

[62] Ibid.

[63] *Certain Activities Carried Out by Nicaragua*, *supra* note 43, para. 104.

[64] ICJ Advisory Opinion on Climate Change, *supra* note 41, para. 299.

to protect natural sites of outstanding universal value[65]; the Ramsar Convention mandates the conservation and wise use of wetlands of international importance[66]; and the CBD requires national biodiversity strategies, sustainable use of biological resources, and both in situ and ex situ conservation measures.[67] These obligations often translate into zoning restrictions, licensing controls, or limits on resource-intensive activities in sensitive areas. Articles 10 and 14 of the CBD explicitly link biodiversity protection to environmental assessment, embedding EIAs within treaty-based conservation duties.[68]
Digital infrastructures intersect with these obligations in several ways. Large data-centre campuses may be sited near wetlands, forests, or coastal zones due to land availability or cooling needs. Upstream mineral extraction for servers, batteries, and cooling systems can drive habitat loss, water depletion, and pollution in biodiversity-rich regions such as the Congo Basin, the Andean highlands, or Indonesian rainforests.[69]

Similar tensions have emerged internationally. Several states - including Singapore, Ireland, and the Netherlands - have introduced moratoria or stricter planning controls on new data-centre developments due to concerns about land availability, biodiversity impacts, and grid capacity.[70] These measures illustrate that treaty-based biodiversity obligations and sustainability principles can have practical implications for digital infrastructure deployment.

2. Obligations to Tackle Climate Change

The United Nations Framework Convention on Climate Change (UNFCCC), the Kyoto Protocol, and the Paris Agreement form the core of the international legal framework

---

[65] Convention for the Protection of the World Cultural and Natural Heritage (adopted 16 November 1972, entered into force 17 December 1975) 1977 UNTS 151, arts. 4–5.

[66] Convention on the Conservation of Wetlands of International Importance Especially as Waterfowl Habitat, (adopted 2 February 1971, entered into force 21 December 1975) 996 UNTS 245, arts. 2–4.

[67] Convention on Biological Diversity (adopted 5 June 1992, entered into force 29 December 1993) 79 UNTS 1760, art. 1.

[68] Convention on Biological Diversity, *supra* note 67, art. 14. See also Convention on Environmental Impact Assessment in a Transboundary Context (adopted 25 February 1991, entered into force 10 September 1997) 1989 UNTS 310.

[69] See e.g., Raid, Afrewatch, *Beneath the Green A critical Look at the Environmental and Human Costs of Industrial Cobalt Mining in DRC*, March 2024, available at https://raid-uk.org/wp-content/uploads/2024/03/Report-Beneath-the-Green-DRC-Pollution-March-2024.pdf; E.S. Rentier, C. Hoorn, A.C. Seijmonsbergen, 'Lithium Brine Mining Affects Geodiversity and Sustainable Development Goals' (2024) 202 *Renewable and Sustainable Energy Reviews* 114642, M. G.Y. Lo et al., 'Nickel Mining Reduced Forest Cover in Indonesia but had Mixed Outcomes for Well-Being' (2024) 7 *OneEarth* 2019.

[70] Data Center Knowledge, *Singapore Ends Data Center Pause As It Seeks Sustainable Growth*, 26 July 2023, available at https://www.datacenterknowledge.com/cooling/singapore-ends-data-center-pause-as-it-seeks-sustainable-growth; D. Swinhoe, *Ireland's Energy Regulator Proposes Policy Requiring Data Centers to Match Load with New Power Generation*, DCD, 19 February 2019, available at https://www.datacenterdynamics.com/en/news/irelands-energy-regulator-proposes-policy-requiring-data-centers-to-match-load-with-new-power-generation/; M. Gooding, *The Ongoing Impact of Amsterdam's Data Center Moratorium*, DCD, 24 August 2024, available at https://www.datacenterdynamics.com/en/analysis/the-ongoing-impact-of-amsterdams-data-center-moratorium/.

governing climate change.[71] The UNFCCC provides the foundational architecture, establishing as its 'ultimate objective' the stabilization of GHG concentrations at a level that prevents dangerous anthropogenic interference with the climate system.[72] The Kyoto Protocol operationalised this objective through binding emissions targets for developed states[73], while the Paris Agreement extends mitigation and adaptation obligations to all Parties through nationally determined contributions (NDCs).[74]

The ICJ has interpreted these instruments as forming a coherent normative framework. Article 2 of the UNFCCC sets the overarching purpose of the climate regime, while Article 4(1) requires all Parties to formulate and implement mitigation measures.[75] The Paris Agreement advances these obligations by requiring states to prepare, communicate, and maintain NDCs reflecting their highest possible ambition.[76] Although the content of NDCs is nationally determined, the Court has clarified that their ambition is constrained by the temperature goals of the Paris Agreement and by general principles of IEL, including the no-harm rule.[77]

Due diligence in implementing climate obligations requires states to adopt legislative, administrative, and enforcement measures, as well as to monitor their effectiveness.[78] Adaptation obligations under Article 7 of the Paris Agreement similarly require states to strengthen resilience and reduce vulnerability on the basis of the best available science.[79] The Court emphasised that these obligations apply irrespective of whether emissions-intensive activities are carried out by public or private actors.[80]

As shown in Section 2, digital infrastructures - including data centres, high-performance computing facilities, and cryptocurrency mining operations - generate GHG emissions through electricity consumption, backup power systems, and upstream supply chains. In some cases, these emissions are comparable to those of established industrial sectors.[81] Digital infrastructure emissions therefore fall within the scope of states' climate obligations under international law, even where they are not explicitly identified as a separate category within national climate policies.

[71] United Nations Framework Convention on Climate Change (adopted 9 May 1992, entered into force 21 March 1994) 1771 UNTS 107; Kyoto Protocol to the United Nations Framework Convention on Climate Change (adopted 11 December 1997, entered into force 16 February 2005) 2303 UNTS 148; Paris Agreement (adopted 12 December 2015, entered into force 4 November 2016) 3156 UNTS 79.
[72] United Nations Framework Convention on Climate Change, *supra* note 71, art. 2.
[73] Kyoto Protocol to the United Nations Framework Convention on Climate Change, *supra* note 71, art. 3.
[74] Paris Agreement, *supra* note 71, art. 3.
[75] ICJ Advisory Opinion on Climate Change, *supra* note 41, para. 197.
[76] Ibid para. 242.
[77] Ibid para. 245.
[78] Ibid paras. 245–246.
[79] Ibid para. 258.
[80] Ibid para. 252.
[81] See generally C. Mora et al., 'Bitcoin Emissions Alone Could Push Global Warming Above 2 C' (2018) 8 *Nature Climate Change* 931.

3. Public Participation and Access to Environmental Information

Public participation and access to environmental information are well-established components of IEL.[82] Principle 10 of the Rio Declaration affirms that environmental issues are best handled with the participation of all concerned citizens, and that individuals must have access to information, opportunities to participate in decision-making, and access to judicial and administrative remedies.[83] Earlier instruments, including the Stockholm Declaration and Agenda 21, similarly recognise access to environmental information as a prerequisite for sustainable development.[84]

These principles are given concrete legal form in regional instruments such as the Aarhus Convention and the Escazú Agreement.[85] The Aarhus Convention establishes three interrelated rights: access to environmental information, public participation in decision-making, and access to justice.[86] Under Article 6, the public must be afforded early and effective opportunities to participate in decisions on activities likely to have significant environmental effects, at a stage when all options remain open.[87] The Escazú Agreement similarly guarantees access to information, participation, and justice in environmental matters, with particular emphasis on land-use planning and activities with significant environmental impacts.[88]

These participatory guarantees apply in principle to any activity capable of affecting the environment. As demonstrated in Section 2, digital infrastructures may generate environmental pressures related to land use, water consumption, and emissions. Decisions concerning their siting, expansion, or operation therefore fall within the range of activities for which public participation and access to environmental information under international and regional environmental instruments may be relevant.

4. Assessing Gaps in the Application of International Environmental Law to Digital Infrastructures

The analysis in Section 3 demonstrates that the principles of IEL are, in principle, applicable to the environmental impacts of digital infrastructures. These principles are activity-based, technology-neutral, and capable of evolving in response to new forms of harm. Yet their application to digital infrastructures exposes a set of structural limitations

[82] P. Sands, J. Peel, *Principles of International Environmental Law* (CUP, 4ed 2018), at 708.
[83] Rio Declaration on Environment and Development, *supra* note 59, Principle 10.
[84] UN Conference on Environment and Development, Agenda 21, UN Doc A/CONF.151/26/Rev.1, 1992, para. 23.2.
[85] UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (adopted 25 June 1998, entered into force 30 October 2001) 2161 UNTS 447 [Aarhus Convention]; Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean (adopted 4 March 2018, entered into force 22 April 2021) [Escazú Agreement].
[86] Aarhus Convention, *supra* note 85, arts. 4–9.
[87] Aarhus Convention, *supra* note 85, art. 6.
[88] Escazú Agreement, *supra* note 85, arts. 5–8.

that go beyond problems of enforcement or political will. As mapped in Section 2, digital activities are transboundary, highly mobile, and deeply embedded in global supply chains. They depend on complex energy and water systems, generate geographically dispersed emissions, and are often operated by private actors who control key technical information These features challenge several procedural and informational assumptions on which IEL relies. To illustrate this, the section examines three interrelated areas in which the operation of existing rules becomes strained: the attribution of environmental effects under the no-harm rule, the assessment of impacts through existing EIA practices, and the effective functioning of cooperation obligations in a sector characterised by technical opacity and private control over data. Taken together, these dynamics reveal structural gaps that complicate the effective operation of IEL in the digital context.

A. The No-Harm Rule and the Problem of Attribution in a Transnational Digital Economy

The no-harm rule presupposes a relatively identifiable relationship between an activity, a territory, and its environmental effects. Although the rule applies to cumulative and indirect forms of harm - including GHG emissions - its preventive logic depends on the ability of states to identify sources of risk, assess their likely impacts, and regulate activities within their jurisdiction or control accordingly.[89]

Digital infrastructures place these assumptions under strain. As demonstrated in Section 2, electricity used to power data centres may be generated in another state; upstream emissions arise in geographically dispersed extraction, manufacturing, and logistics chains; and energy-intensive activities such as cryptocurrency mining may relocate rapidly across borders in response to regulatory or market conditions. Environmental effects are therefore spatially dispersed and temporally fragmented, complicating attribution and weakening the causal visibility between digital activities and environmental harm.

This difficulty is particularly evident in the climate context. Digital infrastructures contribute to cumulative emissions through electricity consumption, backup power systems, and upstream supply chains, yet these contributions are rarely traceable to discrete regulatory decisions or sector-specific activities. As Section 3 has shown, the no-harm rule applies fully to cumulative emissions, but its preventive function depends on informational conditions that enable states to identify foreseeable harm. Where emissions are embedded in general electricity demand, shared grid infrastructures, or globalised production chains, states may lack the data necessary to determine the contribution of digital activities to transboundary environmental effects.[90]

---

[89] *Corfu Channel case*, *supra* note 43, para. 22. Generally, see J. Brunnée, 'Harm Prevention' in L. Rajamani, J. Peel (eds.) *The Oxford Handbook of International Environmental Law* (Oxford, 2nd edn 2021), at 273.

[90] P. Dhar, 'The Carbon Impact of Artificial Intelligence' (2020) 2 *Nature Machine Intelligence* 423; A. P. Victorio, E. Celeste, A. Quintavalla 'Greening AI? The New Principle of Sustainable Digital Products and Services in the EU' (2024) 61 *Common Market Law Review* 1019, at 1040.

The challenge becomes more visible when the no-harm rule is operationalised through the architecture of the international climate regime. The UNFCCC and the Paris Agreement apply to emissions associated with digital infrastructures, and states are required to reflect their highest possible ambition in their NDCs.[91] NDCs thus constitute a primary vehicle through which the duty of prevention is implemented at the national level. Yet the structure of national GHG inventories on which NDCs are based makes it difficult to render digital emissions visible as a distinct category of environmental risk. Emissions linked to data centres, high-performance computing, and cryptocurrency mining are not reported as 'digital' emissions but are dispersed across electricity generation, industrial production, and transnational supply chains. As a result, digital emissions rarely emerge as identifiable regulatory targets, even where they fall within states' jurisdiction or control.

The principle of CBDRRC introduces an additional layer of complexity. The environmental footprint of digital infrastructures correlates strongly with the geographic concentration of data centres, the distribution of mining operations, and the organisation of global value chains. States with advanced digital economies may therefore bear a disproportionate share of responsibility for emissions that are not easily isolated within national inventories. Conversely, states hosting energy-intensive mining operations may experience significant environmental pressures while lacking the regulatory capacity, technical expertise, or informational access necessary to integrate these activities effectively into their climate commitments. While CBDRRC allows for differentiation in the level of obligation, it does not resolve the underlying challenge of attribution and visibility on which preventive regulation depends.

Taken together, these dynamics illustrate that the operation of the no-harm rule relies on monitoring, attribution, and information-sharing mechanisms developed for activities with clearer territorial anchors and more stable production patterns. Digital infrastructures represent an extreme case of cumulative environmental harm: contributions are diffuse, indirect, and often invisible within national inventories, yet foreseeable in light of available scientific evidence. The difficulty, therefore, lies not in the absence of legal obligations, but in the erosion of the conditions that allow those obligations to be meaningfully discharged.

B. Environmental Impact Assessments and the Invisibility of Digital Environmental Harm

EIA is a central procedural mechanism through which the duty of prevention and due diligence is operationalised. In principle, large-scale digital infrastructures - particularly hyperscale data centres and energy-intensive mining facilities - are capable of triggering this obligation.

[91] A. F. D. Luminari, 'Artificial Intelligence and Climate Change: Legal Challenges and Opportunities for Ocean Protection' (2021) 12 *Iura & Legal Systems* 15, at 20.

In practice, however, EIAs rarely capture the environmental footprint of digital infrastructures in a comprehensive manner. This reflects three interrelated limitations. First, digital infrastructures are not consistently recognised as environmentally significant activities under either customary or treaty-based frameworks. Data centres are often categorised as commercial or technological facilities rather than as resource-intensive installations, while cryptocurrency mining operations may be authorised through expedited or fragmented permitting regimes. As a result, activities with substantial land, water, and energy impacts may escape systematic environmental scrutiny. This is particularly relevant in the context of biodiversity treaties, which require assessment of activities likely to affect ecosystems of high ecological value but rarely treat digital infrastructures as falling within this category.[92]

Second, where environmental assessments are conducted, their scope is often narrowly defined. Assessments tend to focus on localised impacts such as noise, traffic, or construction disturbance, while overlooking upstream and system-level pressures. These include emissions embedded in electricity generation, cross-border electricity sourcing, water stress associated with cooling systems, and cumulative effects arising from the clustering of facilities or the expansion of grid infrastructure.[93] Such omissions are difficult to reconcile with the requirement, affirmed in Section 3, to consider indirect, cumulative, and long-term effects where activities contribute to climate change or resource depletion. They also conflict with treaty-based obligations under the CBD, which explicitly link biodiversity protection to environmental assessment, and with public-participation guarantees under the Aarhus Convention or the Escazú Agreement, which presuppose access to comprehensive environmental information.[94]

Third, the sustainability metrics commonly used in the digital sector provide only a partial picture of environmental performance. Indicators such as Power Usage Effectiveness (PUE) focus primarily on energy efficiency within facilities and offer little insight into water consumption, the carbon intensity of electricity, hardware lifecycles, or upstream resource extraction.[95] A facility may therefore appear efficient according to sector-specific benchmarks while generating significant emissions or exacerbating local water stress. Reliance on such metrics limits the substantive value of environmental assessment and constrains the informational basis for public participation.[96]

The invisibility of digital environmental harm also affects the transboundary dimension of assessment. As shown in Section 2, the clustering and mobility of digital infrastructures can generate cumulative pressures on electricity grids and water systems that extend

[92] UNCTAD, Digital Economy Report 2024: Shaping an Environmentally Sustainable and Inclusive Digital Future, UNCTAD/DER/2024, at 22.
[93] OECD, Measuring the Environmental Impacts of AI Compute and Applications: the AI Footprint, OECD Digital Economy Papers, November 2022 No. 341, at 22.
[94] See e.g., Convention on Biological Diversity, *supra* note 67, arts. 12, 14; Aarhus Convention, *supra* note 85, arts. 6, 9; Escazú Agreement, *supra* note 85, arts. 3, 4.
[95] Monstadt, Saltzman, *supra* note 2, at 771.
[96] Ibid.

beyond national borders. In the absence of mechanisms capable of aggregating impacts across facilities, jurisdictions, or timeframes, environmental assessments systematically underestimate the scale of harm associated with digital infrastructures. This points to the need for cross-border and strategic forms of assessment capable of capturing system-level effects.

C. Cooperation, Opacity and the Limits of State Due Diligence

The duty to cooperate is indispensable in addressing environmental harms that are transboundary, cumulative, or systemic in nature. Digital infrastructures generate precisely such effects: their electricity demand is embedded in interconnected grids, their water use affects shared basins, and their supply chains span multiple jurisdictions. Effective prevention therefore depends on cooperation, including information exchange regarding electricity sourcing, grid carbon intensity, water consumption, siting decisions, and upstream resource use.

In practice, cooperation in this domain remains limited, largely due to the opacity of the digital sector and the concentration of critical information in private hands.[97] Cloud infrastructures are designed to be geographically and operationally inconspicuous, and operators frequently treat data on energy contracts, water withdrawals, hardware lifecycles, and supply-chain impacts as commercially confidential.[98] In several jurisdictions, data centre development has proceeded under favourable tax regimes or streamlined permitting processes, further restricting access to environmental information by regulators and neighbouring states.[99] More broadly, digitalisation strategies often remain disconnected from the material constraints that underpin them.[100]

This informational asymmetry constrains the operation of the duty to cooperate as articulated in Section 3. Cooperation presupposes that states have access to the data necessary to assess environmental risks, notify potentially affected states, and coordinate preventive measures.[101] Much of the information required to quantify emissions and resource use in the digital sector is held by private operators rather than public authorities.[102] As a result, large technology companies increasingly function as *de facto* environmental governance actors: through procurement standards, energy purchasing

[97] L. du Toit, 'Artificial intelligence, the earth system, and the law' (2025) *Law, Innovation and Technology* (advanced access publication), at 11.

[98] J. Holt, P. Vonderau, 'Where the Internet Lives': data centers as cloud infrastructure' in L. Parks, N. Starosielski (eds.), *Signal Traffic: Critical Studies of Media Infrastructure* (University of Illinois Press, 2015), at 74.

[99] P. Brodie, 'Climate Extraction and Supply Chains of Data' (2020) 42 *Media, Culture & Society* 1095.

[100] L. E. Bridges, Competing Digital Capacities: between State-led Digital Governance and Local Data Center Tradeoffs (2024) 27 *Information, Communication & Society* 1906.

[101] A. Brett, 'Information as Power: Democratizing Environmental Data' (2022) 2022 *Utah Law Review* 127, at 129, 139–142.

[102] The World Bank and ITU, *Measuring the Emissions & Energy Footprint of the ICT Sector* (The World Bank and International Telecommunication Union, 2024), at 5.

agreements, internal reporting practices, and voluntary sustainability commitments, they shape emissions profiles across global supply chains.[103]

While such private initiatives may support mitigation efforts, they also complicate the allocation of responsibility under IEL. Where key environmental data and decision-making processes remain internal to private entities, states may struggle to obtain the information necessary to design and implement effective regulatory measures, including nationally determined contributions.[104] In these circumstances, states may be unable to determine whether digital activities create foreseeable transboundary effects or whether notification and consultation obligations are triggered.[105]

In this sense, digital infrastructures reveal a structural constraint on the duty to cooperate. Without enhanced transparency and institutionalised mechanisms for information sharing, states face significant obstacles in coordinating responses to the environmental impacts of digitalisation.

5. Fragmentation and the Need to Strengthen Transnational Environmental Governance

The foregoing analysis reveals that the environmental governance of digital infrastructures is marked by significant fragmentation. Existing legal and institutional frameworks were not designed to regulate infrastructures that are highly mobile, technically opaque, and embedded in transnational energy systems and global supply chains. As demonstrated in Sections 3 and 4, the core principles of IEL are formally applicable to digital activities, yet their practical operation remains constrained because the procedural and informational conditions on which they depend are only partially met in the digital context.

IEL is therefore not normatively deficient. Its principles are sufficiently broad and flexible to encompass digital environmental harm. The difficulty lies instead in the misalignment between the transnational, data-intensive, and **privately operated nature of digital infrastructures** and the state-centred mechanisms through which environmental obligations are implemented. The challenge is thus not to construct an entirely new legal regime, but to close the gap between the normative reach of existing principles and their current modes of application. While the negotiation of a comprehensive new treaty on digital environmental impacts may be politically unrealistic, more immediate progress can be achieved through targeted reforms that address the specific sources of fragmentation identified above. Three priorities stand out.

[103] In detail, see G. Pickren, 'The Global Assemblage of Digital Flow': Critical Data Studies and the Infrastructures of Computing (2018) 42 *Progress in Human Geography* 225.

[104] L. Amoore, 'Cloud Geographies: Computing, Data, Sovereignty' (2018) 42 *Progress in Human Geography* 4, at 9.

[105] F. Libertson, J. Velkova; J. Palm, 'Data-center Infrastructure and Energy Gentrification: Perspectives from Sweden' (2021) 17 *Sustainability: Science, Practice and Policy* 152, at 158; S. Farmer, 'The Stone in the Cloud: Planning the Resource Demands of the Data Centre Industry through Land Use Law' (2023) 56 *UBC Law Review* 435, at 483.

First, digital infrastructures should be systematically integrated into climate transparency and reporting frameworks. This would enable states to account more accurately for emissions associated with data centres, high-performance computing, and cryptocurrency mining, including upstream and, where appropriate, Scope 3 emissions. The development of standardised methodologies for measuring digital energy use, water consumption, and lifecycle impacts would enhance comparability and accountability across jurisdictions.[106] Such methodologies could be elaborated within existing institutional settings - including the UNFCCC, the International Telecommunication Union (ITU), and the OECD - without requiring new treaty instruments.[107]

Second, EIA practices must be recalibrated to reflect the cumulative and transboundary nature of digital environmental harm. This entails broader scoping of assessments to include grid-level emissions, water basin impacts, and upstream supply-chain effects, as well as the use of strategic and, where appropriate, cross-border assessments for clusters of data centres and energy-intensive operations.[108] Strengthening public participation and access to environmental **information is central to this effort**, particularly given the technical opacity of digital infrastructures and the concentration of relevant data in private hands. Existing regional frameworks, such as the Aarhus Convention, provide a legal basis for enhancing transparency and participation in decisions concerning digital infrastructure siting and expansion.[109] Domestic reforms already offer instructive examples, including the EU Energy Efficiency Directive, which mandates waste heat recovery for large facilities unless technically or economically unfeasible.[110]

Third, given their control over infrastructure design, energy sourcing, and global supply chains, major digital companies occupy a pivotal position in shaping environmental outcomes. **Binding environmental due diligence obligations** could help align private governance practices with public environmental objectives.[111] Requiring operators to identify, prevent, and mitigate environmental risks across their operations and value

[106] OECD, Recommendation of the Council on Digital Technologies and the Environment, adopted on 8 April 2010, amended on 4 July 2025, OECD/LEGAL/0380.
[107] At the EU level, the AI Act requests providers to display energy consumption information in the technical documentation of AI systems. See Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, Art. 11 together with Annex IV.
[108] Luminari, *supra* note 91, at 20.
[109] T. Le Goff, 'Environmental Law's Principles Applied to Artificial Intelligence: a Path Towards Regulation' (2025) International Review of Law, Computers and Technology (advanced access publication), at 15–16.
[110] Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency and amending Regulation (EU) 2023/955 (recast), OJ L 231/1.
[111] See e.g., Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting, OJ L 322/15; Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, OJ L, 2024/1760. See Scott, Gehring, *supra* note 24.

chains would translate international environmental principles into concrete compliance duties.[112] Emerging practices - such as certified recycling partnerships and adherence to e-waste regimes like the EU Waste Electrical and Electronic Equipment (WEEE) Directive - already point towards a circular economy approach to digital infrastructures, one that can reduce emissions while addressing resource depletion and waste.[113]

Overall, the task is not to reinvent IEL, but to render its existing principles operational in a domain where environmental effects are dispersed, cumulative, and mediated through private infrastructures. In this context, the work of international standard-setting bodies such as International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), which have developed technical standards on energy management, environmental performance, and sustainable digital infrastructure, assumes particular importance.[114]

Their technical standards on energy management, environmental performance, and sustainable digital infrastructure can guide and strengthen the domestic implementation of international environmental obligations. While formally non-binding, the ICJ has emphasised that, in evaluating environmental risks and the content of due diligence obligations, current standards must be taken into consideration.[115] Making IEL effective in the digital context therefore requires a recalibration of procedural tools, enhanced transparency, and the systematic integration of environmental obligations into the governance practices of the actors that design and operate digital systems.

6. Conclusion

Digital infrastructures have become essential to contemporary societies, yet their environmental footprint remains strikingly underexamined in international legal debates. This article has shown that the material foundations of digitalisation produce environmental pressures that are significant, cumulative, and increasingly transboundary. These impacts challenge the persistent assumption that digital technologies are immaterial or inherently sustainable and demand a more deliberate engagement with the ecological dimensions of digital development.

IEL offers a valuable starting point for such engagement. Its core principles are flexible, technology-neutral, and capable of addressing new forms of environmental harm. Treaty-based obligations relating to biodiversity, sustainable development, and climate change further reinforce the relevance of existing frameworks. Yet the practical

[112] Le Goff, *supra* note 109, at 16.
[113] Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) Text with EEA relevance, OJ L 197/38.
[114] International Telecommunication Union, Recommendation ITU-T L.1300, Series L: Construction, Installation and Protection of Cables and Other Elements of Outside Plant. Best Practices for Green Data Centres, June 2014.
[115] *Gabčíkovo-Nagymaros Project*, *supra* note 47, para. 140; ITLOS Advisory Opinion on Climate Change, *supra* note 60, para. 285; ICJ Advisory Opinion on Climate Change, *supra* note 41, para. 287.

application of these principles to digital infrastructures reveals structural limitations: the transnational operation of data centres and mining facilities complicates attribution; the invisibility of digital environmental impacts undermines measurement, reporting, and assessment; and the fragmentation of governance across environmental, digital, energy, and trade regimes leaves key issues outside any coherent regulatory framework.

These challenges do not render IEL irrelevant. Instead, they expose gaps that cannot be closed simply by re-interpreting existing principles. A more coordinated and integrated approach is required - one that recognises digital infrastructures as environmental actors and brings their material impacts within the scope of environmental governance.

Several pathways for such an approach already exist. Incorporating digital infrastructures into climate-transparency frameworks would allow states to account for digital emissions in national inventories and mitigation strategies. Expanding the use of cross-border environmental impact assessments could address the transboundary dimensions of data-centre clusters and mining operations. Strengthening soft-law standards on energy efficiency, water use, cooling technologies, and hardware lifecycles would promote convergence across jurisdictions. Enhanced environmental due-diligence obligations for digital companies and mining operators could improve accountability. And deeper institutional cooperation among environmental, digital, and energy bodies would help bridge existing governance gaps.

Ultimately, the environmental footprint of digitalisation is neither marginal nor inevitable. It reflects choices about infrastructure design, energy sourcing, regulatory priorities, and governance models. Ensuring that digital development aligns with broader environmental objectives requires acknowledging these choices and integrating digital infrastructures into the normative and institutional architecture of environmental law. As digitalisation accelerates, IEL will play an increasingly important role in shaping a sustainable digital future.