T20 Policy Brief

G20 BRASIL 2024

T20 Brasil 2024 Let's rethink the world

Task Force 05

INCLUSIVE DIGITAL TRANSFORMATION

Applying the CII Framework to DPIs: Considerations, Challenges and Opportunities

Manu Misra, Independent Researcher (India)

Jyoti Panday, Researcher, Internet Governance Project (United States)

Nicolo Zingales, Professor of Information Law and Regulation, FGV Rio Law (Brazil)

TF05

Abstract

Crucial towards making digital access more inclusive and public service deliveries more trustworthy, would be a well-rounded understanding of the concept of digital public infrastructure (DPI) on the part of policymakers. Such an understanding would need to be cognizant of the risk of questionable assertions of national security, and its inherent tensions with the developmental aspirations of DPI.

This is particularly so for two reasons. First, DPIs are conceptually overlapping and often legally intertwined with critical information infrastructure (CII), a concept borne from national security policy. Second, there exists an inherent conceptual tension between DPI and CII wherein, the establishment and delivery of DPI values openness, interoperability, and efficiency on one hand, on the other hand CII leans in the opposite direction, towards emphasizing stricter restrictions, controls, and security measures.

In light of this inherent tension between these two concepts that often concurrently provide designations and cause regulatory implications for the same assets, this policy brief provides an insight into what considerations, challenges and gains might arise for policymakers. It does so by citing the development and deployment of DPI and their designations as CII in India particularly. This focus is justified by India's status as an emerging economy where such designations have recently occurred and by the Indian government being a major proponent of the DPI concept in recent years.

The policy brief's recommendations are aimed at the G20 forum and consensus amongst its members would be crucial for a global impact on the issue. However, its core arguments would be relevant to all states aiming to modernize their DPI policy frameworks.

Keywords: critical information infrastructure, digital public infrastructure, national security, public service delivery, digital inclusivity, India0.

Diagnosis of the issue

Global interest in DPI is expanding rapidly, presenting both risks and opportunities for policymakers. The central challenge posed by the regulatory overlap and conceptual tension between DPI and CII can be framed as two related questions: First, which DPI-related assets should be designated and protected as CII? Second, at what point should such designations be made so as to minimize any detrimental impact on development?

As to the first question, it is worth noting that CII is defined in India by the National Critical Information Infrastructure Protection Centre (NCIIPC) as a "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety." It is conceptually the digital subset of a much wider notion of critical national infrastructure (CNI), which traditionally was focused primarily on the security of physical assets but has been vastly expanding its virtual realm in recent years.

While official definitions of CNI tend to vary across jurisdictions, broadly, the term tends to cover assets, whether physical or virtual, that are considered vital for the functioning of an economy and the loss or disruption of which would lead to severe economic or humanitarian consequences, at a national scale. Energy facilities, international ports and telecom networks are therefore some of the prime examples of assets that are often designated as CNI by policymakers worldwide. However, with the rise of the digital economy, the concept may encompass more intangible assets such as platforms, data and related intellectual property, raising more challenges as to their systematic assessment.

Indeed, the debate surrounding CNI has existed for several decades, first with an emphasis on physical security and, with greater technological progress, evolving largely

into a highly technical field, focusing on cyber security and more recently also 'economic security.' For example, usage of the term "critical infrastructure" in recent years has expanded rapidly in the context of foreign investment screening mechanisms in many G20 states (Mildner and Schmucker, 2021)

For an evidence-based identification of CII, the notion of 'criticality' must be recognised as a distinct concept, one that is objectively measurable by the relative dependency of an economy on a certain asset towards its *functioning*. Relative dependency on an asset by other networks within the same sector, and indeed within other sectors, is also a key contributing factor that boosts an asset's criticality.

Criticality here therefore is linked to the impact on the functioning of an economy if a DPI asset were to be lost or disrupted. These assets may include both physical DPI assets such as server/data centers or intangible ones such as the data that DPIs generate or the software that they are supported by. While avoiding high relative dependency on a single DPI asset/segment may not always be feasible, being wary of 'DPI criticality' would help in reducing transaction costs (for both state and private participants) and also in limiting excessive/indiscriminate CII designations.

The second question relates to timing i.e. *when* a certain DPI asset should be designated as CII, specifically whether it may be done *ex-post*, as in *after* the DPI was already developed and scaled, or whether it should ideally be done *ex-ante* at the conceptualization stage itself, before development and scaling.

In India, where the IT Act 2000 under Art 70 allows for 'any computer resource which directly or indirectly affects the facility of CII'' to be declared to be a "protected system" [1], *ex-post* designations have been observable, in what appears to be a reactive, piecemeal

[1] "Gazette Notifications for Declaring Computer Resources Relating to Identified Critical Information Infrastructure (CII) Elements of Various Organisations under Section 70 of IT Act, 2000 | Ministry of Electronics and Information Technology, Government of India." Accessed May 31, 2024.

approach. For e.g., the computer resources and systems relating to India's Unified Payments Interface (UPI), to the National Payments Corporation of India (NPCI) and to the Immediate Payment Service (IMPS) were all designated as CII in 2022, several years after their development[2].

Several benefits do arise from the designation of DPI as CII which could positively impact public trust in the digital economy. These include, for instance higher security standards and cybersecurity guidelines pertaining to the monitoring and control of access to CII assets, along with greater deterrence effects from heavier criminal liabilities and fines for rule violators.

However, the *ex-post* application of such regulatory measures may also pose serious challenges for policymakers. Hence, CII designations should ideally be sought *ex-ante*, i.e. at the conceptualization stage itself**,** particularly when designations would entail commercial restrictions in the form of for vendor lock-ins, foreign investment reviews, 'trust-certificates' and nationality-based restrictions on which cybersecurity products DPI asset owners/operators may adopt.

Ultimately, our overall diagnosis is that, while our understanding of DPIs as an evolving concept and how to regulate such a set of shared large-scale digital systems may indeed need to accommodate some concerns and issues associated with traditional critical infrastructure protection, on the other hand, it is also true that adopting a 'CII approach' to DPIs and their designation as such, must be thought through with caution, in terms of both the degree to which the critical label is applied and the manner in which 'critical-DPIs' are regulated.

https://www.meity.gov.in/gazette-notifications-declaring-computer-resources-relating-identified-critical-information.

[2] 4135 GI/2022 The Gazette of India: Extraordinary § (2022).

This is especially true given the potential for the 'securitization' of DPIs: in other words, excessive or abusive forms of designation driven not by evidence and sound reasoning but by rhetoric that may hamper private (especially foreign) participation and ultimately have a negative impact on public trust in the digital economy.

Recommendations

Recommendation - 1

In light of the above, we recommend that G20 members should work towards building consensus, or at least mutual understandings, on standard definitions, common principles (Saxena and Mahan, 2023), and baseline security guidelines related to CII-related assets and services, along with a universally adaptable 'criticality criteria' that provides an analytical framework to estimate an asset's degree of criticality, thereby allowing policymakers to distinguish critical from non-critical segments of a DPI more easily. This would help minimize ambivalence and enhance predictability for private participants involved in the construction and maintenance of DPIs. Conversely, it may also allow the state to detect and deal with potential vulnerabilities earlier on.

Recommendation - 2

Given the standards and obligations associated with systems being designated as CII, we also recommend that, as far as possible, policymakers should designate DPI assets as CII *ex ante* i.e., at the conceptualization, construction, or developmental phases of DPIs. Doing so would avoid unnecessary transaction costs and adverse technical and operational design implications for DPI owners and operators. To facilitate this, we further recommend that states support and participate in initiatives that facilitate greater

public-private cooperation on the issue. Doing so may again help policymakers better predict future dependencies and vulnerabilities of DPIs but at the same time, would also provide greater transparency and predictability for owners and operators of DPI assets.

Recommendation - 3

A third recommendation from us at this stage would be to channel CII designation decisions through a procedure/mechanism that is sufficiently transparent and mindful of the underlying values associated with DPIs. To facilitate this, policymakers at the G20, in addition to prioritizing domestic public-private collaborations within their respective countries, could also create channels for further cooperation, especially knowledge transfer/exchange, at the international/multilateral level. This includes exchanges between various state agencies and also between DPI owners/operators and CII authorities from different states.

Scenario of outcomes

Outcome – 1

If states fail to arrive at consensus, or even mutual understandings, on standard definitions, common principles, baseline security guidelines for critical DPIs and an analytical framework to estimate the criticality of DPI assets, the potential consequences that may arise would include:

1. Hindering of private investment and innovation: a lack of predictability and consistency: this would create an avoidable confusion among private players involved in the construction and maintenance of DPIs which consequently would consider such ventures as being riskier.

2. Increased security vulnerabilities for governments: a failure to identify and regulate critical components of DPIs would leave them vulnerable to cyber threats and attacks or make them more susceptible to disruptions and breaches.

3. Interoperability challenges: Inconsistent designations of CIIs among G20 member states could lead to interoperability issues, as different countries may have varying standards and regulations for CIIs. This could create barriers to international market collaborations and hinder cross-border exchanges of information and services.

Outcome - 2

If states fail to designate DPI assets as CII early on in the development phase, the potential consequences that may arise would include:

1. Adverse implications for technical and operational design: Retroactively applying the CII label to DPIs could disrupt their technical and operational design. CII designations typically come with specific security requirements and restrictions, which may not have been considered during the initial development of the DPI. This can lead to additional costs and complexities in retrofitting security measures and may compromise the effectiveness of the infrastructure.

2. Governance and accountability challenges: Retrofitting the CII framework onto existing DPIs can also pose governance and accountability challenges. It may require significant changes to existing DPI governance structures and processes to ensure compliance with CII standards and obligations. This can lead to confusion and inefficiencies in managing and overseeing the DPI, potentially undermining its effectiveness and trustworthiness.

3. Capacity and resource constraints: Extending the CII framework to the DPI ecosystem can pose capacity and resource challenges for member states and other

stakeholders involved in managing and securing CII. Retrofitting DPIs as CIIs would then require additional investments in cybersecurity measures, training, and infrastructure upgrades, which may strain already limited resources.

Outcome - 3

If states fail to ensure transparency, collaboration, and alignment with the underlying values associated with DPIs when designating these systems as CIIs, the potential consequences that may arise would include:

1. Erosion of trust: Failing to ensure transparency and collaboration in the designation of CIIs can lead to a perception of arbitrary or opaque decision-making processes. This can erode trust among stakeholders, including the public, private sector, and international partners, in the management and governance of DPIs.

2. Undermining public-private collaboration: Prioritizing state control over DPI assets through the CII framework without adequate collaboration with the private sector can undermine the effectiveness of public-private partnerships that have been prioritized in the institutional design of DPIs. This can hinder innovation, limit investment, and impede the development of resilient and sustainable infrastructure.

3. Impeding knowledge transfers: Failing to facilitate collaboration and cooperation between public and private stakeholders, as well as between state agencies at national and international levels, can impede knowledge transfer and information sharing critical for addressing emerging threats and vulnerabilities in critical systems. This can leave DPIs more susceptible to cyber-security risks such as data leaks, disruptions, and ransomware.

References

Mildner, Stormy-Annika, and Claudia Schmucker. “Investment Screening: Protectionism and Industrial Policy? Or Justified Policy Tool to Protect National Security?” T20 Italy 2021, September 8, 2021. https://www.t20italy.org/2021/09/08/investment-screening-protectionism-and-industrial-policy-or-justified-policy-tool-to-protect-national-security/.

Saxena, Srishti, and Kaushal Mahan. “Establishing Global Norms to Protect Critical Information Infrastructure.” ThinkTwenty (T20) India 2023 - Official Engagement Group of G20, May 13, 2023.

G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

Let's rethink the world

CEBRI
Rethink Tank

FUNDAÇÃO ALEXANDRE DE GUSMÃO

ipea
Instituto de Pesquisa Econômica Aplicada