Cloud as Critical Infrastructure

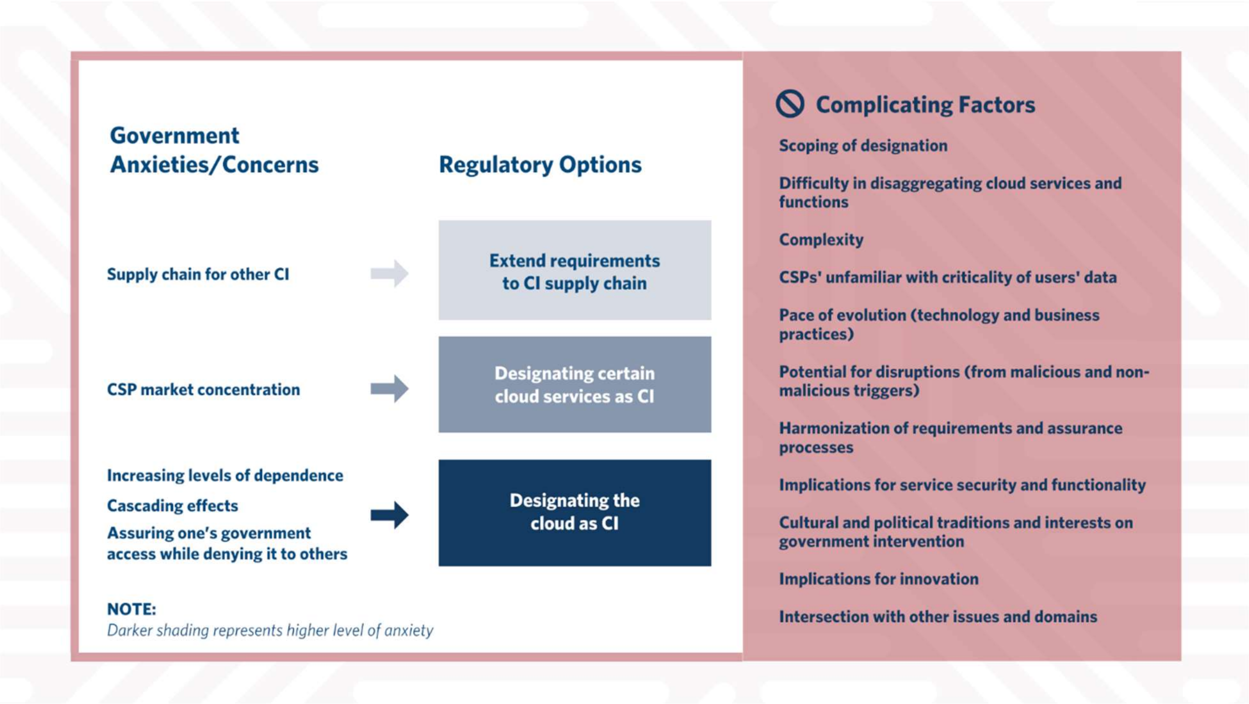
Key Considerations

Government anxieties about cloud market concentration and the surety—understood as the combination of security, robustness, and resilience—of cloud services and providers have increased as cloud-based tools have become more central to the provision of critical and essential services (including public services). One debate that has emerged from this concern is whether and how to designate the cloud industry, or portions of it, as critical infrastructure (CI). For a CI designation to address these anxieties effectively, however, the designation must account for at least the following challenges:

- ***Risk-prioritization and scoping of the CI designation.*** Recognizing how the term “cloud” may refer to different types of providers, services, deployment models, functions, and infrastructures, stakeholders should delineate and narrow the scope of any proposed designation to those aspects of the cloud that are vital to critical services.[1] Narrowing the scope of CI designations becomes increasingly difficult as the cloud evolves, decentralizes, and integrates more deeply with other sectors. For example, as cloud computing moves toward the “edge” and cloud providers integrate with telecommunications providers,[2] it will become more difficult to identify where vital elements of the cloud end and others begin.
- ***Avoid scoping CI designations too narrowly.*** However, taking too narrow an approach to designating the cloud as CI by, for example, focusing on a single provider or one critical customer rather than adopting a sector-wide or systemic outlook, might risk undervaluing the role of the many stakeholders involved in the provision of cloud services, especially in the case of customers who adopt multi-cloud strategies, and the degree of interdependence among them. Moreover, an overly narrow perspective will restrict efforts to ensure that the security and robustness controls in individual critical infrastructure sectors complement and enhance one another.[3]
- ***Moral hazard.*** Governments’ backstopping efforts could lead providers of critical cloud services, enterprise customers who are subject to the critical infrastructure designation, and insurers to be less sensitive to risk because of their increased confidence that the government will support them in the event of a catastrophe. This potentially weakens the incentives for cloud providers and their customers to improve the security and robustness of their systems.
- ***Continuously evolving technology and business practices.*** Defining national requirements and conducting follow-up audits of cloud providers require a significant amount of government attention (in terms of both time and resources). Because

technology and business practices evolve relatively quickly, governments might struggle to keep pace with cloud adoption and innovation. As a result, any CI designation runs the risk of quickly becoming outdated as government agencies may lack the resources to continuously monitor and update requirements in light of new technological developments.

- ***Increased compliance costs.*** As more countries consider designating the cloud as CI, differences between their respective requirements could slow and complicate cloud service adoption and innovation, and create undesirable and conflicting outcomes. Moreover, coupled with other regulatory measures such as data localization requirements, diverging CI requirements could contribute to the fragmentation of the cloud.
- ***Imperfectly accommodating other cloud governance issues.*** CI designations can address security, robustness, and resilience concerns, but might adversely affect issues of consumer and enterprise protection, prosperity and sustainability, and human and civil rights. For example, a CI designation could require the creation of redundant physical infrastructure to improve the robustness and resilience of vital cloud systems but neglect the environmental effects of building and operating it.
- ***Increased potential for government intervention.*** A CI designation may enable increased government intervention, which may in turn adversely affect service functionality, consumer trust, and privacy. As more countries designate the cloud as CI, suspicions will increase about whether some governments have privileged access to cloud services within their jurisdiction, potentially undermining the growth of the international marketplace for cloud services.


Government Anxieties/Concerns
Regulatory Options
Supply chain for other CI
Extend requirements to CI supply chain
CSP market concentration
Designating certain cloud services as CI
Increasing levels of dependence
Cascading effects
Assuring one's government access while denying it to others
Designating the cloud as CI
Complicating Factors
Scoping of designation
Difficulty in disaggregating cloud services and functions
Complexity
CSPs' unfamiliar with criticality of users' data
Pace of evolution (technology and business practices)
Potential for disruptions (from malicious and non-malicious triggers)
Harmonization of requirements and assurance processes
Implications for service security and functionality
Cultural and political traditions and interests on government intervention
Implications for innovation
Intersection with other issues and domains

NOTE:
Darker shading represents higher level of anxiety

With these concerns in mind, governments are considering three approaches when designating the cloud as critical infrastructure and imposing new requirements on cloud providers and customers. Listed in order of increasing severity, these are: (1) consider cloud computing as part of the supply chain for existing critical infrastructure (CI); (2) designate particular services (such as healthcare delivery and disaster relief SaaS) as critical because the cloud brings other issues to bear; or (3) designate the cloud itself—understood as the totality of currently available cloud services—as CI. Each of these approaches seeks to address different types of government anxieties and concerns and attempts to reconcile some complicating factors, such as the difficulties associated with critical cloud components and data, given high levels of cloud integration with other sectors and cloud providers' lack of familiarity with the criticality of their users' data. Regardless of the approach, governments must clearly identify and harmonize the governmental authorities and requirements that may flow from such a designation. Doing so will help to minimize the number of redundant or potentially incompatible requirements, which could have adverse impacts on cloud security and functionality.

Potential Ways Ahead

Recognizing that governments are increasingly unable to understand and audit a cloud provider's performance and operations, regulators should consider borrowing lessons learned from other fields such as banking, aviation, and aerospace, and establish a measurable framework for increasing confidence in the surety of cloud services and their providers.

These requirements (for example, guaranteeing a certain degree of service availability each month) should be developed in collaboration with cloud providers and customers. They should also be tailored for the sector and particular services to which they are being applied and give providers of different services the ability to satisfy the requirements in ways consistent with their unique constraints.

Moreover, these requirements and their accompanying metrics should be designed to ensure that governments have the capacity to effectively audit cloud providers' business practices and operations. This framework also recognizes several options for incentives that could encourage compliance by cloud providers.

- ***Establish performance-based requirements:***
    - Governments should define high-level surety requirements for the confidentiality, integrity, and availability of cloud services and identify metrics by which to measure compliance in consultation with cloud providers and enterprise customers. These may vary based on:
        - Type of service offered (IaaS, PaaS, SaaS)
        - The criticality of the sector (CI and non-CI sectors)
    - Cloud providers should comply with these requirements and, additionally, take the following measures:
        - Implement security and privacy by design.

        - Commit publicly to honor performance-based requirements and provide transparency on compliance with them.
        - Help enterprise customers understand the requirements and meet their responsibilities.
        - Perform system penetration and stress tests and audit compliance internally, adjusting operations as warranted.
    - Governments, cloud providers, and enterprise customers should work together to distinguish between requirements for less and more sensitive workloads, and harmonize these requirements to avoid conflict between them.
- ***Options for incentivizing compliance with performance-based requirements:***
    - Make performance-based requirements a condition for obtaining operational licenses to serve government agencies, CI customers, and other essential functions.
    - Reward cloud providers and their enterprise customers for exceeding the requirements and impose penalties in the event they fail to comply.
    - Make these requirements a condition for obtaining cloud insurance coverage.
    - Consider the use of performance-based requirements as a substitute for prescriptive regulation on cloud security, robustness, and resilience.
    - Work to harmonize these requirements internationally, thereby easing the burden of compliance on cloud providers and enterprise customers.

Recent Examples

- "Big Tech cloud services could face resilience test, says Bank of England," Reuters, 13 September 2021

Notes

[1] For example, is it Google Cloud itself that is vital to servicing the Chicago Department of Transportation's coordinating efforts or is it just Google Maps, an interactive web mapping service that was built using Google Cloud technology, that is integral to the service? Google Cloud, "Chicago Department of Transportation: helping to build a new Chicago," Google, n.d., https://cloud.google.com/customers/chicago-department-of-transportation/.

[2] For more information on edge computing and the cloud's recent evolution, see: Ariel E. Levite, et al., "What is the Cloud?," Carnegie Endowment for International Peace, n.d., https://cloud.carnegieendowment.org/about/background-on-the-cloud/

[3] Larry Gigerich, “The Importance of Energy and ICT Infrastructure in Site Selection as Cloud Computing Broadens”, Ginovus, n.d., https://ginovus.com/the-importance-of-energy-and-ict-infrastructure-in-site-selection-as-cloud-computing-broadens/