

## Government Intervention in Extremis

In times of great peril (such as war or large-scale natural disaster), governments have exercised significant control over major industries, such as raw material production and arms manufacturing, for national security purposes.<sup>1</sup> With the growth of the cloud and the increasing intensity and frequency of cyber attacks, governments may wish to exercise similar control over a major cloud provider and direct its remediation following a major cloud incident.<sup>2</sup> But such interventions may also be sought by governments for political objectives.

### Key Considerations

- ***Unclear conditions for and approaches to government intervention.*** While some governments have insisted on their right to take over or otherwise directly intervene in cloud services, there are no precedents for actually doing so. And uncertainty persists regarding the circumstances (for example, type and intensity of threats to national security) that might warrant or trigger direct<sup>3</sup> government intervention. There is also significant ambiguity about the nature of such interventions (such as the duration, degree,<sup>4</sup> and process of intervention). As a result, such a right to intervene, if exercised, could complicate rather than ease providers' recovery efforts. It also opens the possibility for governments to intervene for other security purposes, including to conduct offensive operations or otherwise gain strategic advantage. Additionally, it may be unclear which government agencies would directly intervene in providers' operations. There may also be uncertainty regarding the standards and procedures for terminating direct government intervention once the initial rationale for it ceases to be valid (for example, following the neutralization of a threat).
- ***Security concerns may complicate intervention arrangements.*** Governments' lack of familiarity with cloud providers' operations and systems may cause them to mismanage recovery efforts, extending outages and disrupting services more broadly and for longer periods than would be the case under the control of cloud providers themselves

## Stakeholder Perspectives

### Government

- Some seek the authority to assume control over cloud providers or to direct providers to work with government agencies in cases of clear threats to national security.
- Some may wish to establish very strict conditions for takeover, lest it reduce confidence in the domestic cloud market and undermine confidence in the stability of their domestic business environment.
- Virtually all oppose other governments' efforts to intervene if it grants them access to sensitive personal, commercial, technical, and other data that could implicate national security, competitiveness, or the privacy of their citizens.

### Providers

- Oppose or resist government takeover in all but the most extreme conditions, where providers themselves are entirely unable to recover from a major incident.
- Support the implementation of considerable oversight and restrictions on any potential direct government intervention (in terms of duration, independent authorization, and more).

### Customers

- May welcome government intervention if it enables the quick and efficient restoration of cloud service.
- Object to interventions that provide governments unfettered access into personal or commercially sensitive data or broadly restricts access and services.
- 

### Others

- N/A


## Tensions with Other Cloud Governance Issues

- **Security and Privacy in Lawful Government Access, Privacy Protections, and Restricting Exports of Cloud Services to Human Rights Violators:** Government intervention could enable a new mode of government access to data otherwise protected by warrant requirements. Additionally, if governments do not secure their modes of access, intervention could leave providers vulnerable to intrusions by other actors.
- **Effects of Cloud Market Concentration:** Preferential government intervention, for example by supporting the recovery of hyperscale providers to the exclusion of smaller/nascent providers, may reinforce existing market inequities.

## Potential Ways Ahead

Government	Providers	Customers	Others
<ul style="list-style-type: none"> <li>• Establish working groups between governments, providers, and enterprise customers to delineate clear “disaster level” thresholds necessary to trigger government intervention as well as the process by which such intervention takes place and the circumstances under which it would conclude. (Shared with cloud providers and enterprise customers.)</li> <li>• Create accountability mechanisms whereby providers and customers may</li> </ul>	<ul style="list-style-type: none"> <li>• Work with governments to ensure customer data is protected in the event of intervention. (Shared with customers.)</li> <li>• Implement technical fail-safes that ensure government intervention does not compromise the security of cloud services.</li> <li>• Ensure enterprise customers are insured against potential abuse or data mismanagement in cases of intervention. (Shared with enterprise customers.)</li> </ul>	<ul style="list-style-type: none"> <li>• Work with cloud providers or third-party insurers to ensure sensitive data is protected against potential abuse or mismanagement in the event of government intervention. (Shared with cloud providers.)</li> <li>• <i>Enterprise customers:</i> Ensure they are insured against potential abuse or data mismanagement in cases of intervention. (Shared with cloud providers.)</li> <li>• <i>Enterprise customers:</i></li> </ul>	<ul style="list-style-type: none"> <li>• N/A</li> </ul>

- ensure that governments do not overstep or abuse their intervention mandate.
  - Create intervention requirements and established agreements among governments, providers, insurers, and other stakeholders to allocate liabilities and responsibilities in the event of intervention.
  - Coordinate agency roles in the event of intervention.
  - Increase cooperation with providers and enterprise customers by mandating joint preparedness exercises. (Shared with cloud providers and enterprise customers.)
  - Coordinate with foreign governments and the appropriate cloud providers or enterprise customers to ensure that citizen privacy, national security, and defense are not at risk of
    - Participate in working groups between governments, providers, and enterprise customers to delineate clear “disaster level” thresholds for government takeover and eventual release. (Shared with governments and enterprise customers.)
    - Increase cooperation with governments and enterprise customers by participating in joint preparedness exercises. (Shared with governments and enterprise customers.)
- Participate in working groups between governments, providers, and enterprise customers to delineate clear “disaster level” thresholds for government takeover and eventual release. (Shared with governments and cloud providers.)
- *Enterprise customers:* Increase cooperation with governments and providers by participating in joint preparedness exercises. (Shared with governments and cloud providers.)



compromise in the event of takeover.

## Recent Examples


- The Australian Government’s Security Legislation Amendment (Critical Infrastructure) Bill 2020. For additional information, see: “[Government Assistance](#),” Australian Government Department of Home Affairs.

## Notes

<sup>1</sup> Anshu Siripurapu, “What is the Defense Production Act?” Council on Foreign Relations, January 26, 2021, <https://www.cfr.org/in-brief/what-defense-production-act>.

<sup>2</sup> “There may be even more limited circumstances where Government identifies an immediate and serious cyber threat to Australia’s economy, security or sovereignty (including threat to life). In these situations, it may be appropriate for Government to declare an emergency. Further, it may also be appropriate for an alerting system at the national level, similar to the current National Terrorism Threat Advisory System, particularly for a cyber-related attack or incident. In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national interest. These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow Government to assist entities take technical action to defend and protect their networks and systems.” (Emphasis in original). See: Australian Government, “Protecting Critical Infrastructure and Systems of National Significance,” Australian Government, Department of Home Affairs, August 2020, <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf> and Australian Government, Critical Infrastructure – Government Assistance in Practice Diagram,” Australian Government, Department of Home Affairs, n.d., <https://www.homeaffairs.gov.au/reports-and-pubs/files/ci-government-assistance-in-practice.pdf>.

<sup>3</sup> For example, the Australian Government has stated that “In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national interest.” (Emphasis in original). See: Australian Government, “Protecting Critical Infrastructure and Systems of National Significance,” Australian Government, Department of Home Affairs, August 2020, <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>.



<sup>4</sup> Extensive government intervention might be unnecessary when limited access to data or cloud operations might suffice.