UNIDIR

Funded by
the European Union

RESEARCH BRIEF

Cloud Computing Governance

FEDERICO MANTELLASSI AND GIACOMO PERSI PAOLI

About this brief

This research brief is a shorter version of a full report, “Cloud Computing and International Security: Risks, Opportunities and Governance Challenges” published by UNIDIR’s Security and Technology Programme. The full report is divided into two parts: a technology primer that gives an overview of major applications of cloud computing with relevance to international security, along with their associated risks and opportunities; and a governance primer that analyses the governance challenges of cloud computing and its arms control implications.

This research brief summarizes key elements of the full report, with a stronger focus on the governance primer. It is structured in four sections. Section 1 provides a brief overview of the technology. Section 2 presents the main governance challenges linked to cloud computing in the context of international security and their implications. Section 3 lays out the implications of cloud computing for arms control. Finally, Section 4 sets out the main conclusions of the full report.

This brief does not detail the full analysis, nor does it present the full research. For a more detailed analysis of the international security risks and opportunities of cloud computing, its intersection with artificial intelligence, as well as a complete analysis of governance challenges and implications of arms control, the reader should refer to the full report.

Authors

Federico Mantellassi

Researcher in the Security and Technology Programme at UNIDIR

Dr. Giacomo Persi Paoli

Head of UNIDIR’s Security and Technology Programme

Citation

Federico Mantellassi and Giacomo Persi Paoli, *Cloud Computing Governance: a Research Brief* (Geneva: UNIDIR, 2024).

© Photo: Cover: Shutterstock/Gorodenkoff. Design and layout by Kathleen Morf.

Contents

1. What is cloud computing?

Cloud computing is a technology that provides people and organizations with on-demand access to a shared pool of configurable computing resources—such as servers, storage, applications and services—that can be quickly provisioned and released over the Internet.[1] Cloud computing is a "system of systems" whose core elements can be deployed in various configurations, with services delivered according to different models.

These **core elements** include virtualization, on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. **Deployment models** are the specific environments and ways in which cloud services are made available to users. They determine how resources are allocated, who has access to them, and how the cloud infrastructure is managed and owned. **Service models** denote the type of service that is delivered to users. Figure 1 visualizes the key components, deployment and service models of cloud computing. Table 1 gives an overview of key differences between cloud computing and traditional computing.

Unlike traditional on-premises information technology (IT) infrastructure, cloud-based architectures do not require organizations to own, maintain or secure resources such as servers, storage systems, networking hardware or even specialized applications.[2] Instead, these resources are provided by a third-party cloud service provider (CSP), which manages the underlying remote infrastructure, enabling users to focus on application deployment and data management. Cloud computing is an essential component of modern IT infrastructure, enabling much of today's global connectivity and digital innovation. For example, cloud computing has now become a key enabler for development of artificial intelligence (AI), supporting the deployment of AI at scale and providing the infrastructure necessary for continuous improvement of AI models.

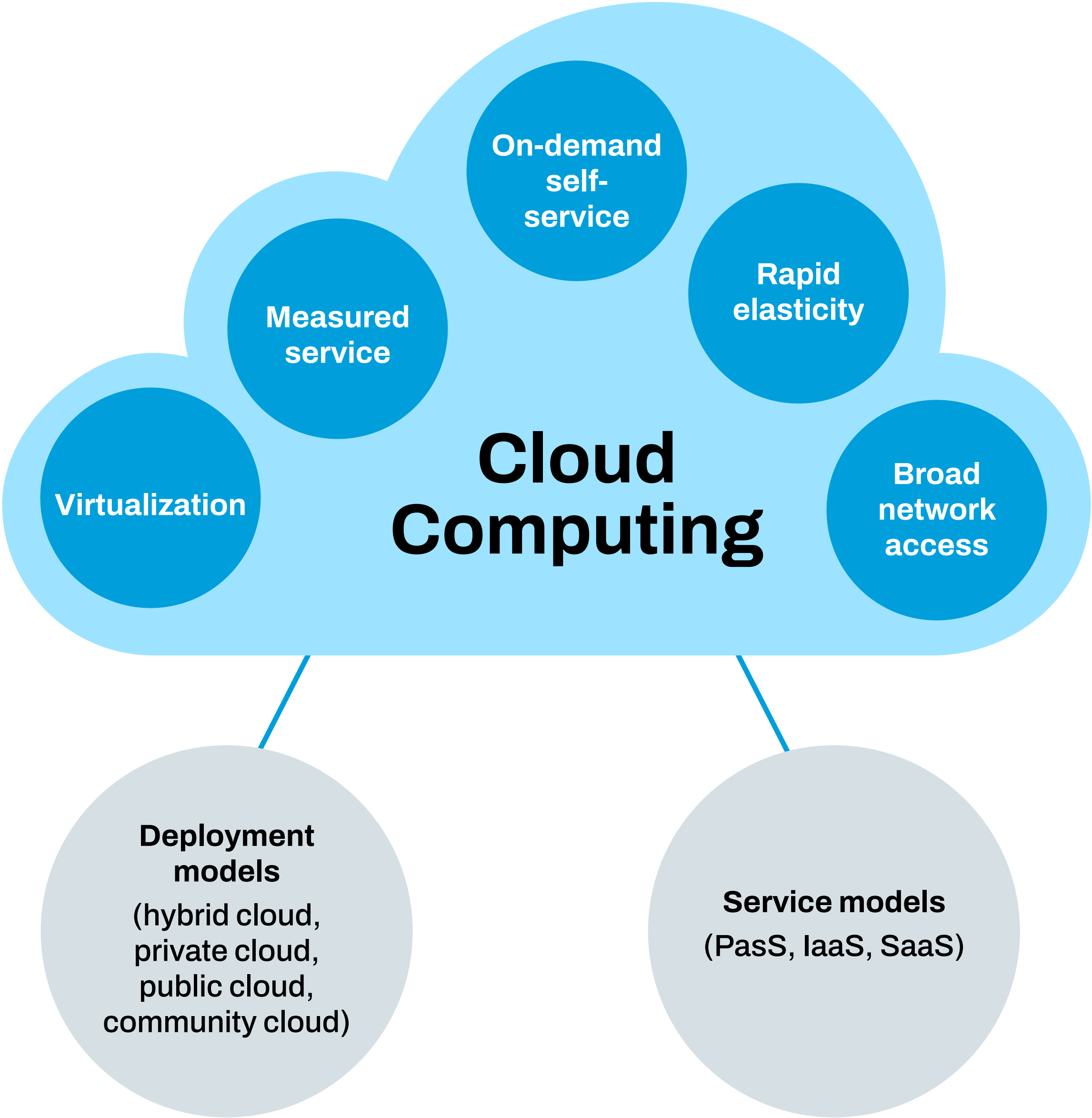
Table 1. Cloud versus traditional computing: overview of main differences

	TRADITIONAL	CLOUD
Ownership and control	Direct ownership and control of entire IT infrastructure	Owned and managed externally, accessed remotely
Scalability	Less flexible and automated, driven by hardware and manual input	Full elasticity, adjusting resources based on demand
Cost model	Capital expenditure	Operational expenditure
Maintenance, security and upgrade	Reliance on dedicated on-premises IT staff	Outsourced to CSPs

[1] Peter M. Mell and Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology (NIST), 28 September 2011, https://doi.org/10.6028/NIST.SP.800-145.

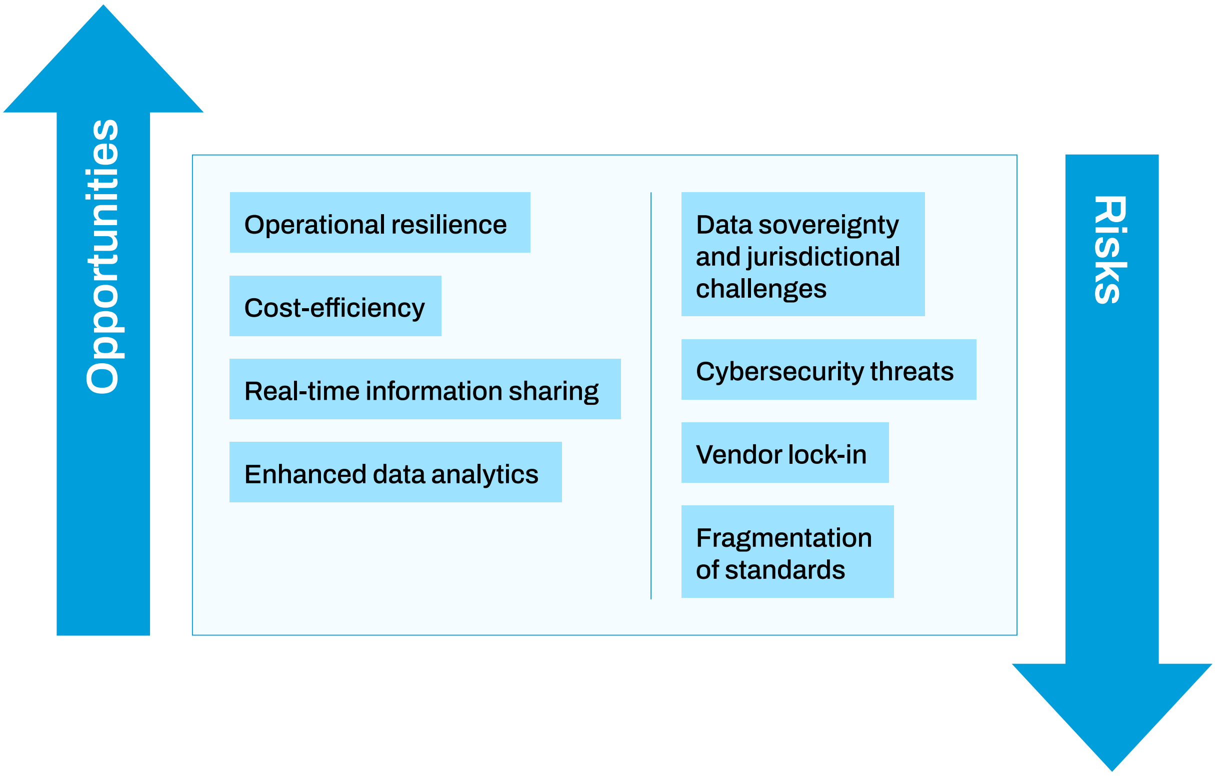
[2] Nishant Kumar, "Cloud Computing vs Traditional Infrastructure: A Comparison", Marvsoft, 1 January 2024, https://marvsoft.co/blog/view/cloud-computing-vs-traditional-it-infrastructure-a-comparison.

Figure 1. The key components and deployment and service models of cloud computing



Today, cloud computing plays a critical role in many sectors that intersect with international security. These range from defence and military operations to national critical infrastructure, as well as humanitarian operations. While cloud computing offers valuable opportunities and benefits including the potential to enhance international security through improved data management, operational efficiency and collaboration – it also carries some challenges and risks. Figure 2 provides an overview of some of the risks and opportunities of cloud computing in the context of international security.

Figure 2. The international security opportunities and risks of cloud computing



See the full report for a full description of the opportunities and risks of cloud computing and their implications, as well as a list of cloud computing applications relevant to international security.

2. Governance challenges in the context of international security

Cloud computing has become a critical enabling technology and important underlying layer of the global digital economy, with implications for international peace and security. It follows that its good governance is key to maximizing the benefits of the technology while minimizing its risks. However, a cohesive, global discussion of cloud computing governance has yet to emerge. Due to some important challenges, the cloud computing governance landscape has instead been fragmented, inconsistent and highly complex. These challenges stem from the nature of the technology itself and the business model behind cloud computing, as well as factors linked to the geopolitical and international security realities with which cloud computing intersects.

The complexity of cloud computing entails that it is a particularly difficult system of technologies to regulate. This has led to a complex regulatory landscape of overlapping policies, legislation, best practices and standards across sectors, industries and countries. While the reach of cloud computing is global, **it exhibits extremely high levels of geographical and market concentration**. This has an important effect on governance by conferring on a few industry players strong influence over regulatory, technological and governance discussions.

Additionally, as technologies do not exist in silos, **cloud computing intersects with governance discussions of other technologies** (e.g., subsea cables, microchips and AI). This not only means that it is difficult to devise a cohesive, focused effort around cloud computing, but also that cloud computing is both a set of technologies to govern and a technology whose governance can be used in the service of the governance – and policy goals – of another set of technologies. This is especially true in the context of the governance of AI. Furthermore, cloud computing is deeply interwoven with states' desires to reduce their dependence on foreign technology and to limit the flow of data outside their territories. This has put **digital sovereignty** considerations at the heart of discussions surrounding cloud computing governance and has had a substantial impact on the shape of the cloud computing landscape. Lastly, there are governance and legal **challenges linked with the increased use of cloud computing by armed forces to deliver warfighting capabilities** as well as with the **delivery of services by CSPs in conflict scenarios**.

The governance of cloud computing brings to light the tensions inherent to an increasingly interconnected global digital environment, and the seemingly competing requirements of national security. This is further exacerbated by growing importance of digital technologies and connectivity, and the global technology competition resulting from it. A more cohesive global approach to cloud computing governance and the coordination of governance approaches, frameworks and tools would be advisable. Further fragmentation of the governance landscape could adversely affect cloud security, safety and resilience, and reduce the ability of the international community to reap the benefits of cloud computing while addressing its risks.

Table 2 provides a brief description of each of these challenges and sets out their implications. A comprehensive and more in-depth analysis of each challenge and its implications can be found in the full report.

Table 2. Challenges of cloud computing governance and their implications

GOVERNANCE CHALLENGE	DESCRIPTION OF THE CHALLENGE	IMPLICATIONS FOR CLOUD COMPUTING GOVERNANCE
Complexity	The "cloud" comprises an intricate network of technologies (both hardware and software), services and actors operating on a global scale across sectors. As such, it is a complex system of systems of technologies that exhibits high levels of opacity, where clearly understanding the relationships between its various elements and clearly identifying risk-nodes is particularly difficult.	• Regulatory and governance complexity, inconsistency, difficulty and fragmentation • Complex landscape to navigate for companies and government policymakers enforcing cloud regulation and governance • Large number of actors and mandates across sectors, technologies and jurisdictions • Heavy compliance burden on CSPs • Potential negative impact on cloud security, safety and resilience
Geographical and market concentration	Despite its global, networked and complex nature, cloud computing exhibits extremely high levels of market concentration. The 10 largest CSPs are concentrated in three countries, and the top 3 capture 65 per cent of the global market.	• Concentrated influence over the technology and its governance among few private companies • Knowledge imbalance between private sector and government regulators • Opacity in functioning and security practices of CSPs • Contributes to the centrality of digital sovereignty in governance discussions
Intersection with other technology governance efforts	Cloud computing intersects with a host of other international governance discussions and efforts, such as those on subsea cables, AI, microchips, 5G and 6G communications, or broader Internet and cyberspace governance. The deep embedding of cloud computing within the broader AI governance discussion is of particular note. Indeed, an emergent discussion in AI governance places cloud computing as a tool in the AI governance toolbox. These proposals seek to govern certain aspects of AI – mainly access to computing power and microchips – *through* the cloud.	• Overlap with other governance discussions and efforts • Influence of adjacent governance discussions, efforts and actions on cloud computing landscape • Growing need for cross-fertilization between governance efforts across technological fields

Table 2. continued

GOVERNANCE CHALLENGE	DESCRIPTION OF THE CHALLENGE	IMPLICATIONS FOR CLOUD COMPUTING GOVERNANCE
Digital sovereignty	Digital sovereignty lies at the heart of governance discussions of cloud computing. This has principally been the result of the geographical concentration of major CSPs in a few states, the cross-border nature of cloud computing, the perceived risk of foreign influence, and the economic and national security importance of data in the 21st century. For these reasons, cloud computing has found itself in the crosshairs of states' desires to minimize their dependence on foreign technology, and to limit the flow of data from their territories.	• Increased regulatory fragmentation • Entwinement with geopolitical competition • Differing data privacy and security standards across states and regions • Increased compliance burden on CSPs • Potential negative impact on other governance goals • Important shaper of the cloud computing landscape
Increased use in the military domain	The increased use of cloud computing solutions in the military domain, and by actors involved in national security in a broader sense, not only has international security implications but presents governance challenges as well. The increased use of cloud computing by armed forces to deliver warfighting capabilities has direct implications. There are also governance challenges linked to the provision of digital services by CSPs in times of conflict.	• Blurred line between military and civilian technology • Growing centrality, dependence on, and influence of technology firms in conflicts and military affairs • Implications for international humanitarian law and cascading effects on civilian persons and infrastructure • Furthers desire for digital sovereignty, increases difficulty of cooperation

3. Implications for arms control

The implications of cloud computing extend to the field of arms control for two main reasons. First, cloud computing is increasingly a key method through which digital, intangible and dual-use capabilities are stored, shared, and accessed. These capabilities are also developed through remote access to large amounts of computing power. Second, much of the world's digital infrastructure now relies on the functioning and integrity of cloud computing services.

This entails two key goals for arms control in the context of cloud computing:

1. **Protecting the cloud**: Cloud computing and its related infrastructure forms a critical layer of society and the economy and is an enabler of digital connectivity and digital innovation. It should therefore be protected.
2. **Developing "digital twins" of arms control concepts for the cloud**:[3] Cloud computing can be used to access and develop digital capabilities or move and access digital information subject to arms control provisions. Arms control mechanisms should thus give the international community the ability to effectively monitor the cloud's use in this way.

Table 3 describes these goals and ways forward.

[3] In the context of this brief, "digital twin" does not refer to a virtual replica of a physical object, but rather an equivalent of arms control tools and mechanisms better suited to the characteristics of the digital world.

Table 3.Cloud computing implications for arms control

PROTECTING THE CLOUD	DEVELOPING “DIGITAL TWINS” OF ARMS CONTROL MECHANISMS
The issue	
Cloud computing is increasingly embedded in all layers of the global economy and is becoming vital to the functioning of critical sectors. Failures, either accidental or as the result of adversarial action, would have dire consequences across society.	The technological realities of cloud computing strain the logic of traditional concepts of arms control and their capacity to be effective. These concepts (e.g., export controls) focus on territoriality and control over physical objects and their movements. As such, they struggle to address the dynamic and borderless flow of data that cloud computing allows or to address the proliferation risk of disruptive AI capabilities enabled by remote access to large amounts of computing power.
A way forward	
Arms control is not limited to the management of weapon systems but is also concerned with behaviours and norms. Hence, a global conversation outlining a common set of expectations, norms and behaviours among states with respect to cloud computing and its related infrastructure should emerge. In the cyber domain, this starts with the implementation of commitments under the framework of responsible state behaviour in the use of information and communication technologies (ICTs). As cloud computing is not just a cybersecurity issue, a similar set of expectations, behaviours and norms surrounding physical attacks on cloud services and infrastructure should be set out. There should also be similar common agreements with respect to armed forces’ use of cloud computing services.	The international community’s ability to meet the arms control challenges of the increased prevalence of cloud computing will largely depend on its ability to develop the “digital twins” of various arms control concepts and mechanisms for the digital world. For export controls for example, this necessitates the development of novel ways of operationalizing “control” in the dematerialized context of cloud computing. This requires understanding which concepts and tools can have greater effect in managing remote access to large amounts of computing power. Further research should explore how other concepts (e.g., licensing requirements) can be applied to this end. Greater international harmonization in this field will also be necessary.

4. Conclusions

The international community should seek to reduce the fragmentation of the governance landscape for cloud computing by better aligning and harmonizing governance approaches. A single catch-all governance framework for cloud computing might not be achievable or desirable. However, greater international coordination and interoperability between governance frameworks will help minimize gaps and contradictions among frameworks. This will help foster a more cohesive global approach that is more conducive to ensuring cloud security, safety and resilience.

A more in-depth understanding and exploration of the impact of cloud computing on arms control is necessary to avoid its unique characteristics being used to further proliferate disruptive dual-use technologies. A multilateral discussion focused on the protection of the cloud is necessary, as well as the development of the "digital twins" of various arms control tools for the realities of cloud computing. This should be complemented by further research into what existing and new tools (e.g., licensing requirements) can be used in the context of arms control for cloud computing. Going forward, this endeavour should not be limited to cloud computing, as novel technologies will continue to strain the effectiveness of the traditional arms control toolbox.

States should deepen discussion on cloud computing in the context of multilateral discussions on international ICT security. This should include an analysis of its unique challenges and the extent to which the existing framework is able to address them. It must also include an analysis of the unique opportunities that cloud computing offers to help states with the implementation of existing commitments and to boost national cyber resilience.

A true multi-stakeholder approach is necessary to discuss, design and implement appropriate policy responses to the challenges of cloud computing. An important – and highly recommended – element of this approach should be the meaningful involvement in such discussions of a geographically representative group of industry players active in this domain. The same applies for representatives of academia, civil society and the technical community, including security researchers and incident responders.

UNIDIR

𝕏 @unidir

in /unidir

/un_disarmresearch

f /unidirgeneva

▶ /unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG