

云计算治理

研究简报

Federico Mantellassi和Giacomo Persi Paoli

关于本简介

本研究简报是联合国裁军研究所（裁研所）安全与技术方案完整报告《云计算与国际安全：风险、机遇和治理挑战》的简短版本。报告全文分为两部分：技术入门概述了云计算与国际安全相关的主要应用及其相关风险和机遇；治理入门分析了云计算的治理挑战及其对军备控制的影响。

本研究简报概述了报告全文的主要内容，重点放在治理入门上。它分为四个部分。第 1 节简要概述了云计算技术。第 2 节介绍在国际安全背景下与云计算相关的主要治理挑战及其影响。第 3 节阐述云计算对军备控制的影响。最后，第 4 节列出了报告全文的主要结论。

本简报不详述全部分析，也不介绍全部研究。如需更详细地分析云计算的国际安全风险和机遇、云计算与人工智能的交叉，以及对军备控制的治理挑战和影响的完整分析，读者应参阅报告全文。

关于作者

Federico Mantellassi 是联合国裁军研究所安全与技术方案的研究员。

Giacomo Persi Paoli 博士是联合国裁军研究所安全与技术方案的负责人。

引用

Federico Mantellassi 和 Giacomo Persi Paoli，《云计算治理：研究简报》（日内瓦：联合国裁军研究所，2024 年）。

1.什么是云计算？

云计算是一种技术，为个人和组织提供按需访问可配置计算资源（如服务器、存储、应用程序和服务）共享池的服务，这些资源可通过互联网快速配置和释放。¹云计算是一个“系统体系”，其核心要素可以通过不同的配置进行部署，并根据不同的模式提供服务。

这些**核心要素**包括虚拟化、按需自助服务、广泛的网络接入、资源池、快速弹性和衡量服务。**部署模式**是向用户提供云服务的具体环境和方式。它们决定了资源的分配方式、资源的访问权限以及云基础设施的管理和拥有方式。**服务模式**表示向用户提供的服务类型。图 1 展示了云计算的关键组件、部署和服务模式。表 1 概述了云计算与传统计算的主要区别。

与传统的企业内部信息技术（IT）基础设施不同，基于云的架构不要求企业拥有、维护或保护服务器、存储系统、网络硬件甚至专门应用程序等资源。²相反，这些资源由第三方云服务提供商（CSP）提供，后者负责管理底层远程基础设施，使用户能够专注于应用部署和数据管理。云计算是现代 IT 基础设施的重要组成部分，为当今的全球互联和数字创新提供了极大的便利。例如，云计算现已成为人工智能（AI）发展的关键推动因素，支持大规模部署人工智能，并为持续改进人工智能模型提供必要的基础设施。

表 1. 云计算与传统计算：主要区别概述

	传统	云
所有权和控制权	直接拥有和控制整个 IT 基础设施	由外部拥有和管理，可远程访问
可扩展性	灵活性和自动化程度较低，由硬件和人工输入驱动	完全弹性，根据需求调整资源
成本模式	资本支出	业务开支
维护、安全和升级	依赖专职的内部部署 IT 人员	外包给云服务提供商

¹Peter M. Mell 和 Timothy Grance，“NIST 对云计算的定义”，国家标准与技术研究院 (NIST)，2011 年 9 月 28 日，<https://doi.org/10.6028/NIST.SP.800-145>。

² Nishant Kumar，“云计算与传统基础设施：比较”，Marvsoft，2024 年 1 月 1 日，<https://marvsoft.co/blog/view/cloud-computing-vs-traditional-it-infrastructure-a-comparison>。

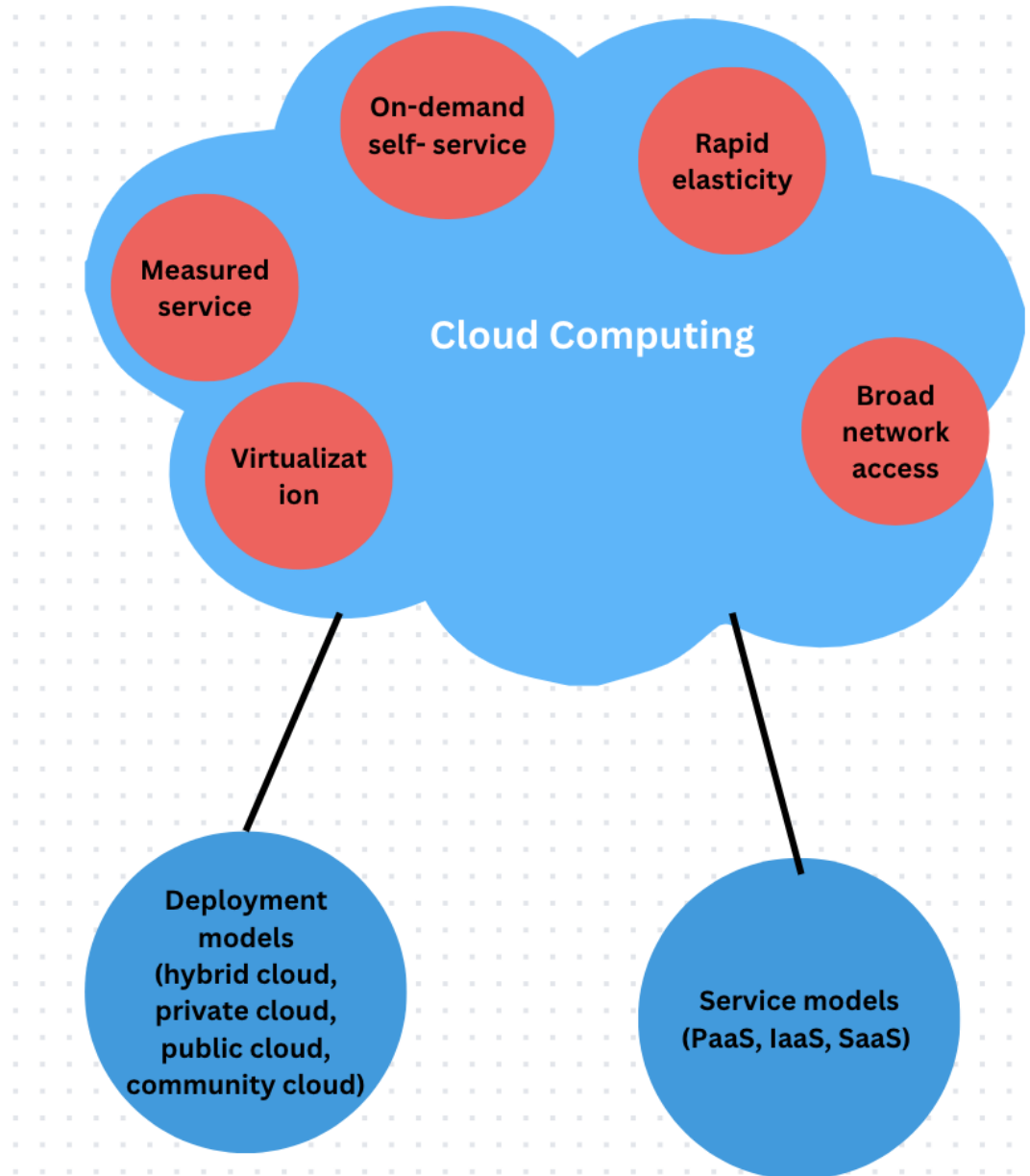


图 1. 云计算的关键组成部分以及部署和服务模式

如今，云计算在许多与国际安全相关的领域发挥着至关重要的作用。这些领域包括国防和军事行动、国家关键基础设施以及人道主义行动。云计算提供了宝贵的机遇和益处，包括通过改进数据管理、运行效率和协作来加强国际安全的潜力，但同时也带来了一些挑战和风险。图 2 概述了云计算在国际安全方面的一些风险和机遇。

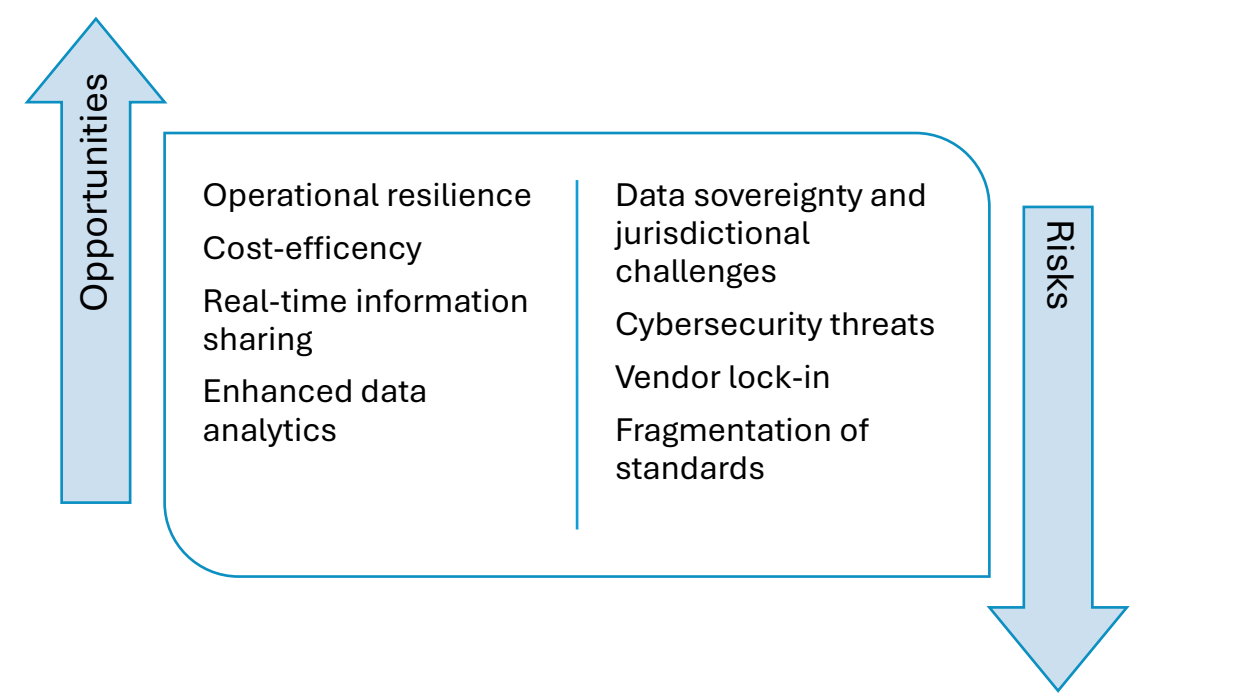


图 2. 云计算的国际安全机遇与风险

有关云计算的机遇和风险及其影响的完整描述，以及与国际安全相关的云计算应用清单，请参阅报告全文。

2.国际安全背景下的治理挑战

云计算已成为全球数字经济的关键使能技术和重要基础层，对国际和平与安全具有影响。因此，良好的云计算治理是最大限度地发挥该技术的优势，同时最大限度地降低其风险的关键。然而，关于云计算治理的全球统一讨论尚未出现。由于一些重要的挑战，云计算治理的格局一直是支离破碎、不一致和高度复杂的。这些挑战源于技术本身的性质和云计算背后的商业模式，以及与云计算交织在一起的地缘政治和国际安全现实相关的因素。

云计算的复杂性决定了它是一个极难监管的技术系统。这导致各部门、各行业和各国的政策、立法、最佳做法和标准相互重叠，形成了复杂的监管格局。虽然云计算的影响范围遍及全球，但其地域

和市场集中度极高。这对治理产生了重要影响，因为少数行业参与者对监管、技术和治理讨论具有强大的影响力。

此外，由于技术并非孤立存在，**云计算与其他技术**（如海底电缆、微芯片和人工智能）的治理讨论相互交叉。这不仅意味着很难围绕云计算开展有凝聚力、有重点的工作，还意味着云计算既是一套需要治理的技术，也是一种技术，其治理可用于为另一套技术的治理和政策目标服务。这一点在人工智能的治理的背景下尤为明显。此外，云计算与国家减少对外国技术的依赖和限制数据在境外流动的愿望紧密交织在一起。这使得**数字主权**问题成为云计算治理讨论的核心，并对云计算格局的形成产生了重大影响。最后，**武装部队越来越多地使用云计算来提供作战能力，以及云服务提供商在冲突情况下提供服务**，也带来了治理和法律方面的挑战。

云计算的治理揭示了日益相互关联的全球数字环境所固有的紧张关系，以及看似相互竞争的国家安全要求。数字技术和连通性日益重要，由此引发的全球技术竞争进一步加剧了这种紧张关系。在云计算治理和协调治理方法、框架和工具方面，最好采用更具凝聚力的全球方法。治理格局的进一步分散可能会对云的**安**保、安全和弹性产生不利影响，并削弱国际社会在应对云计算风险的同时获取云计算效益的能力。

表 2 简要介绍了每项挑战及其影响。对每项挑战及其影响的全面和更深入的分析可参见报告全文。

表 2. 云计算治理的挑战及其影响

治理挑战	挑战描述	对云计算治理的影响
复杂性	“云”由技术（包括硬件和软件）、服务和在全球范围内跨部门运作的行为体组成，是一个错综复杂的网络。因此，“云”是一个复杂的技术系统体系，具有高度的不透明性，要清楚地了解其各要素之间的关系并明确识别风险节点尤为困难。	• 监管和治理的复杂性、不一致性、难度和分散性 • 企业和政府政策制定者在执行云法规和治理时需要应对复杂的局面 • 跨部门、跨技术和跨辖区的大量参与者和任务 • 云服务提供商的合规负担沉重 • 对云安保、安全和弹性的潜在负面影响

地理和市场集中度	尽管云计算具有全球性、网络化和复杂性的特点，但其市场集中度极高。最大的 10 家云服务提供商集中在三个国家，前三名占据了全球市场的 65%。	• 对技术及其治理的影响集中在少数几家私营公司身上 • 私营部门和政府监管机构之间的知识不平衡 • 社区服务提供商的运作和安全做法不透明 • 促进数字主权在治理讨论中的核心地位
与其他技术治理工作的交叉	云计算与许多其他国际治理讨论和努力相互交叉，如关于海底电缆、人工智能、微芯片、5G 和 6G 通信或更广泛的互联网和网络空间治理的讨论和努力。 云计算在更广泛的人工智能治理讨论中的深度嵌入尤其值得注意。事实上，人工智能治理领域正在兴起的一场讨论将云计算作为人工智能治理工具箱中的一个工具。这些建议试图通过云计算来治理人工智能的某些方面——主要是计算能力和微芯片的获取。	• 与其他治理讨论和工作重叠 • 相邻治理讨论、努力和行动对云计算市场格局的影响 • 各技术领域的治理工作日益需要相互促进
数字主权	数字主权是云计算治理讨论的核心。这主要是由于主要的云服务提供商在地理上集中在少数几个国家、云计算的跨境性质、感知到的外国影响的风险以及数据在 21 世纪的经济和国家安全重要性。由于这些原因，云计算已成为各国希望尽量减少对外国技术的依赖和限制数据从其领土流出的目标。	• 监管更加分散 • 与地缘政治竞争的纠葛 • 各州和各区域的数据隐私和安全标准不同 • 增加云服务提供商的合规负担 • 对其他治理目标的潜在负面影响 • 对云计算格局有重要的塑造作用

更多用于军事领域	云计算解决方案在军事领域以及在更广泛意义上参与国家安全的行为体中的使用日益增多，不仅会对国际安全产生影响，还会带来治理方面的挑战。 武装部队越来越多地使用云计算来提供作战能力会产生直接影响。在冲突时期，由云服务提供商提供数字服务也会面临治理方面的挑战。	• 军用技术与民用技术之间的界限模糊不清 • 技术公司在冲突和军事事务中的中心地位、依赖性和影响力日益增强 • 对国际人道主义法的影响以及对平民和基础设施的连带影响 • 促进对数字主权的渴望，增加合作难度
----------	---	--

3.对军备控制的影响

云计算对军备控制领域产生影响主要有两个原因。首先，云计算日益成为存储、共享和访问数字、无形和双重用途能力的关键方法。这些能力也是通过远程访问大量计算能力而发展起来的。其次，目前世界上大部分数字基础设施都依赖于云计算服务的运行和完整性。

这就要求在云计算背景下实现军备控制的两个关键目标：

- 1. **保护云：**云计算及其相关基础设施是社会和经济的重要组成部分，是数字连接和数字创新的推动者。因此，应该对其加以保护。
- 2. **为云计算开发军备控制概念的“数字孪生”：**
³ 云计算可用于获取和开发数字能力，或移动和获取受军备控制规定限制的数字信息。因此，军备控制机制应使国际社会有能力以这种方式有效监控云的使用。

表 3 介绍了这些目标和前进方向。

表 3.云计算对军备控制的影响

保护云	开发军备控制机制的“数字孪生”
-----	-----------------

³在本简介中，“数字孪生”并非指实物的虚拟复制品，而是指更适合数字世界特点的军备控制工具和机制的等同物。

问题：云计算日益深入全球经济的各个层面，对关键部门的运作至关重要。意外或敌对行动导致的故障将给整个社会带来严重后果。	问题：云计算的技术现实限制了传统军备控制概念的逻辑及其有效能力。这些概念（如出口控制）的重点是领土和对实物及其移动的控制。因此，它们难以应对云计算所允许的动态、无边界的数据流，也难以应对远程访问大量计算能力所带来的破坏性人工智能能力的扩散风险。
前进之路：军备控制不仅限于武器系统的管理，还涉及行为和规范。因此，应开展全球对话，概述各国对云计算及其相关基础设施的一套共同期望、规范和行为。 在网络领域，首先要在负责任的国家使用信息和通信技术（ICTs）行为框架下履行承诺。由于云计算不仅仅是一个网络安全问题，因此应围绕对云服务 and 基础设施的物理攻击制定一套类似的期望、行为和规范。还应就武装部队使用云计算服务达成类似的共同协议。	前进之路：国际社会能否应对云计算日益普及所带来的军备控制挑战，在很大程度上取决于其是否有能力为数字世界开发各种军备控制概念和机制的“数字孪生”。 以出口控制为例，这就需要开发新的方法，在云计算的非物质化背景下实施“控制”。这就需要了解哪些概念和工具，可以在管理远程访问大量计算能力方面发挥更大作用。进一步的研究应探索如何将其他概念（如许可要求）应用于这一目的。在这一领域加强国际协调也是必要的。

4.结论

国际社会应通过更好地调整和协调治理方法，努力减少云计算治理环境的分散性。单一的云计算全面治理框架可能无法实现，也不可取。然而，加强治理框架之间的国际协调和互操作性将有助于最大限度地减少框架之间的差距和矛盾。这将有助于形成更具凝聚力的全球方法，更有利于确保云的安保、安全和弹性。

有必要更深入地了解 and 探讨云计算对军备控制的影响，以避免其独特性被用于进一步扩散破坏性的双重用途技术。有必要开展以云计算保护为重点的多边讨论，并针对云计算的现实情况开发各种军备控制工具的“数字孪生”。除此以外，还应进一步研究在云计算军备控制方面可使用哪些现有工具和新工具（如许可证要求）。展望未来，这项工作不应局限于云计算，因为新技术将继续对传统军备控制工具箱的有效性造成压力。

各国应在关于国际信息和通信技术安全的多边讨论中深化关于云计算的讨论。这应包括分析云计算的独特挑战以及现有框架在多大程度上能够应对这些挑战。讨论还必须包括分析云计算为帮助各国履行现有承诺和提高国家网络韧性所提供的独特机遇。

要讨论、设计和实施应对云计算挑战的适当政策，必须采取真正的多利益相关方方法。其中，一个重要且值得强烈推荐的因素应是让活跃在该领域的具有地域代表性的行业参与者有意义地参与此类讨论。这同样适用于学术界、民间社会和技术界的代表，包括安全研究人员和事件响应人员。