UNIDIR

Funded by
the European Union

REPORT

Cloud Computing and International Security: Risks, Opportunities and Governance Challenges

FEDERICO MANTELLASSI AND GIACOMO PERSI PAOLI

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This publication was funded by the European Union as part of UNIDIR's Security and Technology Programme, which is supported by the governments of Czechia, Germany, Italy, the Netherlands and Switzerland, and by Microsoft. The authors wish to thank Sarah Grand-Clément, May-Ann Lim and Dr. Andraz Kastelic for their thoughtful comments on previous versions of this report.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

About the Security and Technology Programme

Contemporary developments in science and technology present new opportunities as well as challenges to international security and disarmament. UNIDIR's Security and Technology Programme aims to build knowledge and awareness about the international security implications and risks of specific technological innovations and convenes stakeholders to explore ideas and develop new thinking on ways to address them.

Note

The designations and material presentation in this publication do not signify any opinion from the Secretariat of the United Nations regarding the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in this publication are the sole responsibility of the individual authors and do not necessarily represent the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Citation

Federico Mantellassi and Giacomo Persi Paoli, *Cloud Computing and International Security: Risks, Opportunities and Governance Challenge*s (Geneva: UNIDIR, 2024).

Authors

Federico Mantellassi

Researcher in the Security and Technology Programme at UNIDIR

Federico's work focuses on the international security implications, risks and opportunities of emerging science and technology developments and innovations. Previously, Federico was a Research and Project Officer at the Geneva Centre for Security Policy, conducting research on the intersection of emerging technologies, international security and warfare. He holds a master's degree in intelligence and international security from King's College London and a bachelor's degree in international studies from the University of Leiden.

Dr. Giacomo Persi Paoli

Head of UNIDIR's Security and Technology Programme

Giacomo's expertise spans the science and technology domain with an emphasis on the implications of emerging technologies for security and defence. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe, where he led the defence and security science, technology and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He holds a doctorate in economics from the University of Rome and a master's degree in political science from the University of Pisa.

Abbreviations

AI	Artificial intelligence
C4ISR	Command, control, communications, computers, intelligence, surveillance and reconnaissance
CSP	Cloud service provider
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service
ICT	Information and communications technology
ISO	International Organization for Standardization
IT	Information technology
OEWG	Open-Ended Working Group

Contents

Executive summary

Cloud computing has become a foundational element of the global digital economy, unlocking unprecedented levels of innovation and connectivity. To understand the profound impacts of this critical enabling technology on international security, this report provides an overview of relevant use cases, benefits and risks of cloud computing, as well as its key governance challenges and implications for arms control. Structured into two parts – a technology primer and a governance primer – this report offers both technical insights and policy analysis.

The technology primer provides an accessible description of the technology, unpacking its various component elements while giving an overview of selected benefits, risks and relevant international security applications. Cloud computing enables scalability and flexibility of computing resources, as well as cost-efficiency and real-time data-processing and sharing. At the same time, it can compound cybersecurity threats, enhance cross-border jurisdiction problems and heighten dependencies on a few large service providers.

The technology primer also situates cloud computing within the broader artificial intelligence (AI) context, underscoring its role in enabling and accelerating AI development. As sectors which intersect with international security – such as defence, critical infrastructure and humanitarian sectors – increasingly adopt cloud computing solutions, careful balancing of risks and benefits is of utmost importance.

In view of this, the governance primer provides an overview of key governance challenges that are relevant in the context of international security. These challenges stem from factors inherent to the technology – and business model – itself, as well as broader factors linked to the geopolitical and international security realities with which cloud computing intersects. The challenges include cloud complexity, digital sovereignty, market and geographical concentration, intersection with other technology governance efforts, and governance challenges of increased use in military domain.

Lastly, this report considers the impact of cloud computing on arms control. It provides a springboard for a discussion of how arms control discussions can better account for the issues brought forth by cloud computing, as well as how traditional arms control mechanisms – such as export controls – are affected by new technological realities.

Introduction

Cloud computing is an essential component of modern information and communications technology (ICT) infrastructure. By allowing relatively affordable access to large amounts of computing power, cloud computing has become a critical enabling technology, powering much of the current unprecedented levels of digital technological innovation and growth.[1] Cloud service providers (CSPs) – which now include "hyperscalers" or large CSPs – bear the upfront cost of constructing and maintaining networks of computing infrastructure (large data centres, power, software, cables, cooling, computers, microchips etc.), and then rent out various services to users for a fee. The use of cloud computing is already prevalent across some sectors, and its importance is only set to increase as the recent artificial intelligence (AI) boom is both enabled by, and reliant on, cloud computing infrastructure and services.[2]

Cloud computing plays a crucial role across sectors that intersect with international security, from defence and national critical infrastructure to humanitarian operations.[3] While providing enormous benefits – from cost-efficiency, strengthened resilience, access to large computational resources, easier data-sharing and analytics – cloud computing also carries potential downsides and risks. The centrality of cloud computing to modern life and the concentration of services among a few actors mean that failures – either accidental or as the result of adversarial action – can be severe, with cascading effects across industries, services and states.[4]

As explored throughout the report, the development of cloud computing in a safe, secure and resilient way is one of the key components of an equally safe, secure and resilient global digital environment. It follows that the good governance of cloud computing at an international level is a key building block to this end.[5]

---

1 Andrew James Lewis, "An Overview of Global Cloud Competition", Center for Strategic and International Studies, April 2023, https://www.csis.org/analysis/overview-global-cloud-competition.

2 Jefferey Erickson, "The Role and Benefits of AI in Cloud Computing", Oracle, 21 June 2024, https://www.oracle.com/sa/artificial-intelligence/ai-cloud-computing.

3 Tianjiu Zuo et al., *Critical Infrastructure and the Cloud: Policy for Emerging Risk* (Washington, DC: Atlantic Council, July 2023), https://dfrlab.org/wp-content/uploads/sites/3/2023/07/critical_infra_and_the_cloud.pdf.

4 Edward Ongweso Jr., "The Microsoft/Crowdstrike Outage Shows the Danger of Monopolization", *The Guardian*, 20 July 2024, https://www.theguardian.com/technology/article/2024/jul/20/the-microsoftcrowdstrike-outage-shows-the-danger-of-monopolization.

5 Maynak Pathak, Kamta Nath Mishra and Satya Prakash Singh, "Securing Data and Preserving Privacy in Cloud IoT-based Technologies: An Analysis of Assessing Threats and Developing Effective Safeguard", *Artificial Intelligence Review,* vol. 57, no. 269 (2024), https://doi.org/10.1007/s10462-024-10908-x.

Furthermore, by multiplying the vectors through which data can be transferred and accessed, and by democratizing access to vast amounts of computing power, cloud computing carries with its implications for arms control and non-proliferation that merit the attention of the disarmament community. A clear understanding of the current governance trends, issues and challenges – from the complexity of the cloud to the impact of digital sovereignty requirements – is thus necessary.

This report is therefore structured in two main parts. First, a **technology primer** sets out what cloud computing is and how it differs from traditional methods of computing. Part 1 also contextualizes cloud computing within the development of AI, exploring the intersection between the two technologies, and unpacks major cloud computing applications with relevance to international security, along with their associated risks and opportunities. Second, a **governance primer** considers the governance implications of cloud computing, emphasizing the need for greater regulatory alignment in the governance of cloud computing in order to maximize effective use of the technology. It sets out major challenges in cloud computing governance and explores implications for arms control.

Part 1. Technology primer

1.1. 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.[6] Unlike traditional on-premises information technology (IT) infrastructure, cloud-based architecture does not require organizations to own, maintain or secure resources such as servers, storage systems, networking hardware or even specialized applications.[7] Instead, these resources are provided by a third-party cloud service provider, which manages the underlying remote infrastructure. This enables the users to focus on application deployment and data management.

The core elements of cloud computing include:[8]

1. **Virtualization:** A single physical hardware system operates multiple virtual instances. Virtualization is crucial for efficient resource allocation and enables the scaling capabilities of the cloud.[9]
2. **On-demand self-service:** Users can access cloud services as needed, without human interaction with the service provider. This feature allows flexibility and rapid provisioning or downscaling of resources.[10]
3. **Broad network access:** Cloud services are accessible from any device with an Internet connection. This supports remote use of resources and collaboration across geographic boundaries.[11]
4. **Resource pooling:** CSPs use a multitenant model – a single cloud instance and infrastructure built to enable multiple cloud customers (tenants) to efficiently share scalable computing resources in a public or private cloud. In a multitenant architecture, each cloud customer's data is kept separate, and tenants are generally unaware of each other's presence.[12] This allows multiple customers to be served with the same physical resources, achieving high levels of efficiency and cost savings.
5. **Rapid elasticity:** Cloud resources scale up or down automatically in response to demand. This provides businesses with the flexibility to handle fluctuating workloads.[13]
6. **Measured service:** Cloud computing operates on a pay-as-you-go model, with usage monitored, controlled, and reported. This allows a user to only pay for the resources that it consumes.[14]

---

6 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.

7 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.

8 For a detailed discussion on the core elements of cloud computing see Mell and Grance, "The NIST Definition of Cloud Computing".

9 Ashish Kumar Dass et al., "Virtualization in Cloud Computing: Transforming Infrastructure and Enhancing Efficiency", *Research and Applications: Emerging Technologies*, vol. 5, no. 3 (2023): 26–40, https://zenodo.org/records/10300506.

10 Cloud Standards Consumer Council, "Practical Guide to Cloud Computing", Version 3.0, December 2017, https://www.omg.org/cloud/deliverables/CSCC-Practical-Guide-to-Cloud-Computing.pdf.

11 World Bank, "Cloud Computing Overview", June 2016, http://documents.worldbank.org/curated/en/837891494407497011/Cloud-computing-overview.

12 Zscaler, "What Is a Multitenant Cloud?", n.d., https://www.zscaler.com/resources/security-terms-glossary/what-is-multitenant-cloud-architecture.

1.2. What are the different types of cloud computing solutions?

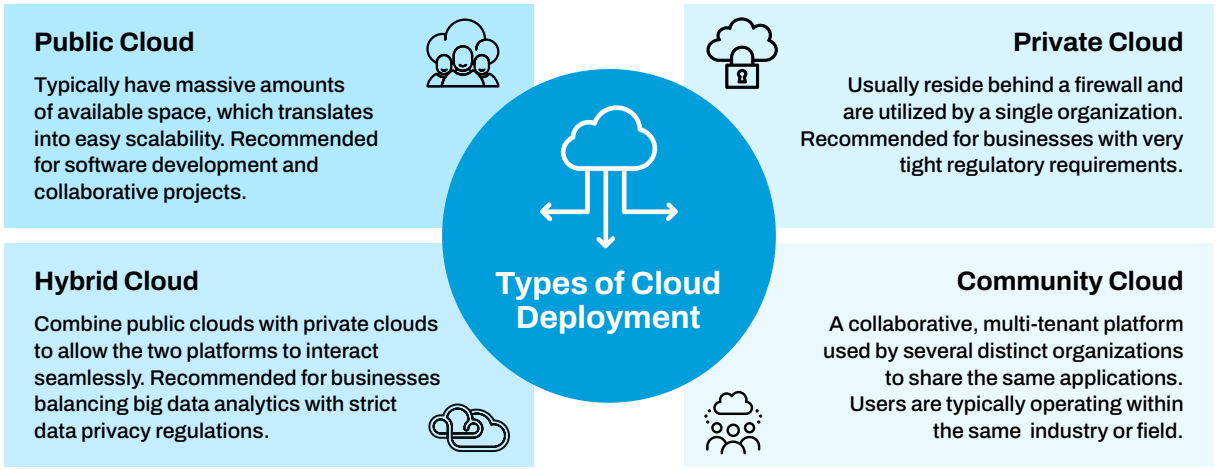
There are two primary ways to categorize cloud computing: based on deployment (or access) or based on type of service provided.[15]

Deployment models

Different deployment models (see Figure 1) have an impact on accessibility and security of data, but also affect costs:

- **Public cloud**: Offered by third-party providers (e.g., Amazon Web Service, Microsoft Azure, Alibaba Cloud) to multiple users. Often the most cost-efficient, but security is a consideration as data is stored in a shared environment.[16]
- **Private cloud**: Exclusively used by a single organization. Provides greater control and security, often at a higher cost.[17]
- **Hybrid cloud**: Combines public and private clouds. Allows an organization to keep sensitive data on a private cloud while leveraging public cloud power for other applications.[18]
- **Community cloud**: A cloud shared by several organizations with similar needs, such as government agencies in allied countries. Fosters collaboration while maintaining security.[19]

Figure 1. Types of Cloud Deployment[20]



13 Yahya Al-Dhuraibi et al., "Elasticity in Cloud Computing: State of the Art and Research Challenges", *IEEE Transactions on Services Computing*, vol. 11, no. 2 (2018), https://doi.org/10.1109/TSC.2017.2711009.

14 Frederic de Vaulx, Eric Simmon and Robert Bohn, "Cloud Computing Service Metrics Descriptions", National Institute of Science and Technology, April 2018, https://doi.org/10.6028/NIST.SP.500-307.

15 N. Rajeswari, "Overview of Cloud Computing and Its Types", *Journal of Emerging Technologies and Innovative Research*, vol. 6, no. 3 (2019), https://www.jetir.org/papers/JETIRAT06008.pdf.

16 Amazon Web Services, "What is a Public Cloud?", n.d., https://aws.amazon.com/what-is/public-cloud.

17 Modebola Olowu et al., "A Secured Private-Cloud Computing System", in *Applied Informatics*, eds Hector Florez et al. (Cham: Springer Nature, 2019), https://doi.org/10.1007/978-3-030-32475-9_27.

18 Cloud Standards Consumer Council, "Practical Guide to Cloud Computing".

19 Alexandros Marinos and Gerard Briscoe, "Community Cloud Computing", in *Cloud Computing*, Lecture Notes in Computer Science no. 5931, eds Martin Gilje Jaatun, Gansen Zhao and Chunming Rong (Berlin: Springer, 2009), https://doi.org/10.1007/978-3-642-10665-1_43.

20 "4 Cloud Deployment Models: Their Advantages and Disadvantages", TurningCloud Solutions, 21 January 2021, https://www.turningcloud.com/blog/cloud-deployment-models.

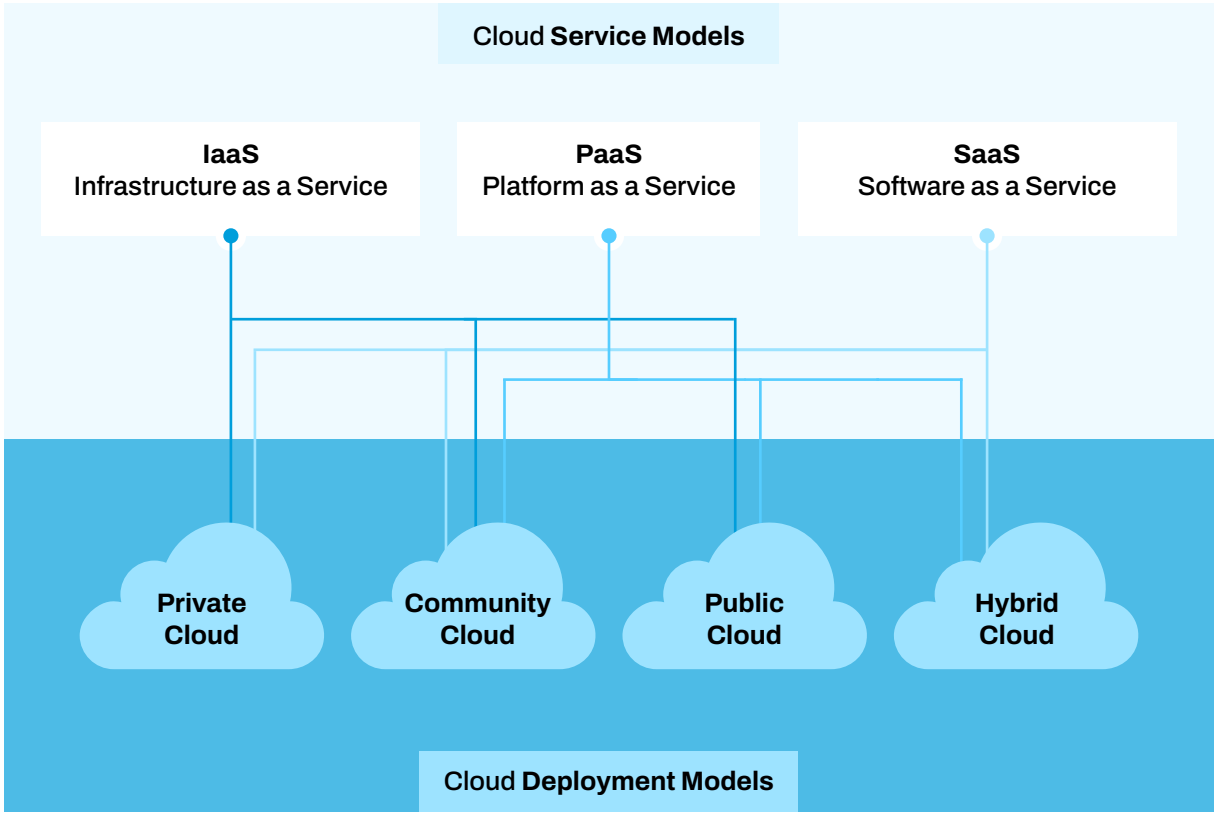
Service models[21]

In addition to the deployment model, cloud computing can also be categorized on the basis of the service that it provides:

- **Infrastructure as a service (IaaS)**: Offers fundamental computing resources such as virtual machines and storage. Users control the infrastructure but rely on the provider for hardware maintenance.[22]
- **Platform as a service (PaaS)**: Provides a platform to build, test and deploy applications, outsourcing infrastructure management to the service provider.[23]
- **Software as a service (SaaS)**: Delivers fully managed software applications directly accessible over the Internet.[24]

Different service models can operate with different deployment models (see Figure 2)

Figure 2. Service models and deployment models[25]



21 Since this primer is meant as an introduction, it only covers the core cloud services. There exist many other "anything as a service" (XaaS) offerings that use and are deployed on different modes and models of cloud computing.

22 Mohammed Suliman, "A Brief Analysis of Cloud Computing Infrastructure as a Service (IaaS)", *International Journal of Innovative Science and Research Technology*, vol. 6, no. 1 (2021), https://www.ijisrt.com/assets/upload/files/IJISRT-21JAN690.pdf; Manishaben Jaiswal, "Cloud Computing and Infrastructure", *International Journal of Research and Analytical Reviews*, vol. 4, no. 2 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772381.

23 Cloud Standards Customer Council, "Practical Guide to Platform-as-a-Service", Version 1.0, September 2015, https://www.omg.org/cloud/deliverables/CSCC-Practical-Guide-to-PaaS.pdf.

24 Lakshmisri Surya, "Software as a Service in Cloud Computing", *International Journal of Creative Research Thoughts*, vol. 7, no. 4 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3674386.

25 Dmitry Koshkin, "Cloud Deployment Models: Advantages and Disadvantages", Sam Solutions, n.d., https://sam-solutions.us/insights/advantages-and-disadvantages-of-cloud-deployment-models.

1.3. How does cloud computing differ from traditional methods of computing?

Cloud computing represents a significant shift from traditional IT infrastructure, which typically involves servers, storage and networking equipment that are managed directly by an organization on its own premises.[25] This set-up requires substantial upfront investment, including for the purchase of hardware and software licences and for dedicated IT personnel for ongoing maintenance.

The differences between cloud and traditional computing can be summarized as follows (see also Table 1):

- **Ownership and control**: In traditional set-ups, an organization owns and directly controls all aspects of its IT infrastructure. With cloud computing, the infrastructure is hosted externally, managed by CSPs, and accessed remotely.[27]
- **Scalability**: Traditional IT infrastructure is generally less flexible and requires manual hardware intervention to scale up or down. In contrast, cloud computing provides elasticity, automatically adjusting resource availability based on demand.[28]
- **Cost model**: While traditional systems usually require upfront capital expenditure for purchasing hardware, cloud computing is often based on an operational expenditure model (i.e., costs are variable and billed according to resource usage).[29]
- **Maintenance, security and upgrades**: On-premises set-ups require dedicated IT staff for maintenance, while CSPs handle infrastructure updates, security patches and hardware upgrades, reducing burdens on the user.[30]

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

26 DMS Technology, "Cloud Computing vs. Traditional On-Site Storage", n.d., https://www.dmstechnology.com/wp-content/uploads/2017/01/Cloud-VS-Traditional.pdf.

27 Mohit Agarwal and Gur Mauj Saran Srivastava, "Cloud Computing: A Paradigm Shift in the Way of Computing", *International Journal of Modern Education and Computer Science*, vol. 12 (2017): 38–38, https://doi.org/10.5815/ijmecs.2017.12.05.

28 Audrey Ingram, "Scalability and Elasticity: Deciphering the Differences in Cloud Computing", Bonsai, 30 August 2024, https://www.hellobonsai.com/blog/scalability-vs-elasticity.

29 Artan Mazrekaj, Isak Shabani and Besmir Sejdiu, "Pricing Schemes in Cloud Computing: An Overview", *International Journal of Advanced Computer Science Applications*, vol. 7, no. 2 (2016), https://thesai.org/Downloads/Volume7No2/Paper_11-Pricing_Schemes_in_Cloud_Computing_An_Overview.pdf.

30 Geeks for Geeks, "Difference between Cloud Computing and Traditional Computing", 23 May 2024, https://www.geeksforgeeks.org/difference-between-cloud-computing-and-traditional-computing.

1.4. What are the main applications of cloud computing relevant to international security?

Cloud computing plays a crucial role across sectors that intersect with international security, from defence and national critical infrastructure to humanitarian operations. Its scalability, resource efficiency and real-time data-processing capabilities make it a powerful tool. Yet it has implications that need careful consideration in areas that have an impact on global stability and safety.

While a full analysis of the benefits and risks associated with each relevant application of cloud computing is beyond the scope of this report, the following subsections provide a brief description of some that are currently being deployed. However, it should be noted that cloud computing is a key enabler of much of modern digital transformation given the increasing computing power requirements. As a result, as the use and diffusion of this technology is continuously evolving, different use cases may emerge in the future.

Defence and military operations

- **Command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR)**: Cloud computing enables rapid data processing and seamless communication across units, thereby enhancing decision-making and operational efficiency. Cloud-based systems allow military forces to share intelligence in real time, coordinate responses and maintain situational awareness across geographically dispersed areas.[31]
- **Cybersecurity operations**: Military organizations increasingly rely on cloud platforms to monitor and defend against cyberthreats.[32] Cloud computing's scalability enables the use of AI in cyber defence and allows for robust data analysis, real-time detection and rapid response to cyber incidents. Additionally, cloud-based cybersecurity frameworks offer tools for the sharing of threat intelligence among allied states, thereby strengthening collective cyber defences.[33]
- **Logistics and supply chain management**: Cloud solutions facilitate better oversight and resilience in logistics, ensuring that supplies and critical resources are available during operations.[34] In an environment where adversaries may target supply chains, cloud-based tracking and data analytics enhance the ability to monitor assets, predict shortages and securely coordinate resupply operations.
- **Data resilience and distributed data storing**: Cloud solutions provide the necessary infrastructure and tools for cyber resilience by effectively distributing government data across various data centres. This helps governments and military organizations adapt to modern conflict scenarios.

---

31 Isabella Healion, "Cloud Computing in Defence", Finabel, July 2024, https://finabel.org/cloud-computing-in-defence.

32 Sally Cole, "Cloud Security for Military Ops: It's Complicated", Military Embedded Systems, 17 October 2016, https://militaryembedded.com/cyber/cybersecurity/cloud-security-for-military-ops-its-complicated.

33 Lauren Zabierek et al., *Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure* (Cambridge, MA: Belfer Center, 2021), https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/8.10.21 Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure.pdf.

34 DataTex, "Cloud Computing Enhances Supply Chain Logistics Capabilities", n.d., https://www.datexcorp.com/cloud-computing-2.

Critical infrastructure protection

- **Energy sector**: Cloud platforms are used to monitor and manage energy-production and distribution facilities and other critical infrastructure in real time.[35] By aggregating data from sensors and control systems, cloud computing enables predictive maintenance, fault detection and resilience planning.[36]
- **Transportation and logistics networks**: Airports, seaports and rail systems increasingly leverage cloud solutions for managing logistics and security.[37] Cloud-based platforms enable predictive analytics to anticipate disruptions and to facilitate real-time coordination across international borders.[38]

Humanitarian sector and disaster response

- **Crisis coordination and aid distribution**: To optimize logistics and ensure that aid reaches those in need, cloud platforms facilitate real-time information-sharing between governments, non-governmental organizations and international organizations.[39] By streamlining communication, cloud solutions reduce redundancies and speed up relief efforts, especially in large-scale crises.
- **Data collection and analysis for conflict zones**: Humanitarian agencies could use cloud resources to collect and analyse data from conflict areas. This can include social media monitoring, satellite imagery and other sources that provide insights into developing situations on the ground.[40] Real-time analysis aids in assessing risk, prioritizing response efforts and guiding international diplomatic efforts to mitigate further conflict.

Beyond the above illustrative examples, other application areas that could be relevant to public safety and national security include health and healthcare as well as intelligence and law enforcement.

---

35 Kenneth P. Birman, Lakshmi Ganesh and Robert van Renesse, "Running Smart Grid Control Software on Cloud Computing Architectures", Cornell University, n.d., https://www.cs.cornell.edu/~lakshmi/Research_files/computational-Needs11smartgrid.pdf.

36 Enrico Zero, Mohammed Sallak and Roberto Sacile, "Predictive Maintenance in IoT-Monitored Systems for Fault Prevention", *Journal of Sensor and Actuator Networks*, vol. 13, no. 5 (2024), https://doi.org/10.3390/jsan13050057.

37 Johannes Kern, "The Digital Transformation of Logistics: A Review About Technologies and Their Implementation Status", in *The Digital Transformation of Logistics: Demystifying Impacts of the Fourth Industrial Revolution*, eds Mac Sullivan and Johannes Kern (New York: John Wiley and Sons, 2021), https://doi.org/10.1002/9781119646495.ch25.

38 Amitabh Verma, "Green Thinking: Impact of Smart Technologies on Supply Chain Management", *Journal of Science and Technology Policy Management*, 2024, https://doi.org/10.1108/JSTPM-01-2024-0020.

39 United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and United Nations Development Programme (UNDP), *Innovation in Disaster Management: Leveraging Technology to Save More Lives* (New York: OCHA and UNDP, May 2023), https://www.undp.org/sites/g/files/zskgke326/files/2024-03/innovation_in_disaster_management_web_final_compressed.pdf; Valerie Lucus-McEwen, "How Cloud Computing Can Benefit Disaster Response", Government Technology, 7 May 2012, https://www.govtech.com/em/disaster/how-cloud-computing-can-benefit-disaster-response.html.

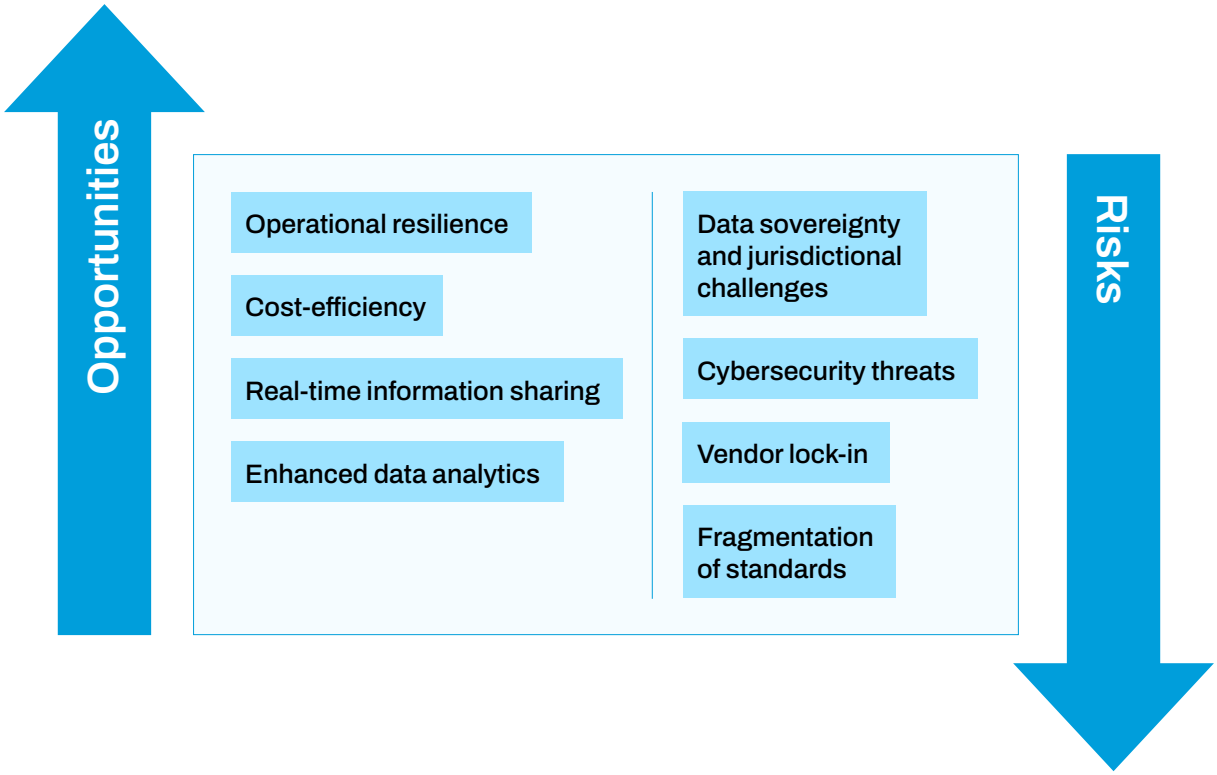
40 Guido Cervone et al., "Using Social Media and Satellite Data Damage Assessment in Urban Areas During Emergencies", in *Seeing Cities Through Big Data*, eds P. Thakuriah et al. (Cham: Springer, 2017), https://doi.org/10.1007/978-3-319-40902-3_24.

1.5. What are the opportunities and risks of cloud computing for international security?

As a bridge between the technical introduction of cloud computing and a deeper analysis of related governance issues, this section presents selected opportunities offered by cloud technology to strengthen security frameworks as well as selected risks and vulnerabilities and their specific implications for international security (see Figure 3 for an overview).

It is clear that cloud computing offers valuable opportunities to enhance international security through improved data management, operational efficiency and collaboration (see Table 2). However, it also carries some challenges and risks, some general that apply to both on-premises and cloud-based architectures and some specific to the cloud (see Table 3).[41]

Figure 3. The international security opportunities and risks of cloud computing



41 A recent World Bank report provides an in-depth analysis of cybersecurity issues related to the cloud. See World Bank, *Unpacking Cloud Cybersecurity: A Guide for Policy Makers in Developing Countries* (Washington, DC: World Bank, 2024). https://documents1.worldbank.org/curated/en/099103124193527496/pdf/P1778521dda0ba08e19fcb1f0d251cdb786.pdf.

Table 2. Overview of opportunities of cloud computing

OPPORTUNITY	DESCRIPTION	IMPLICATIONS
Operational resilience and disaster recovery[42]	Cloud-based systems provide built-in resilience through data redundancy and disaster recovery mechanisms. These allow organizations to quickly restore critical operations following a disruption (whether accidental or intentional).	In the context of international security, cloud resilience improves the ability of governments and organizations to increase their resilience against cyberattacks, natural disasters and other disruptive events. For military operations, this resilience ensures that critical communications and command systems remain functional, even under adverse conditions. For humanitarian missions, cloud-based support for disaster recovery ensures continuity of aid distribution and logistics during crises.
Cost-efficiency and resource optimization[43]	Cloud computing operates on a pay-as-you-go model, allowing organizations to avoid significant capital expenditure and to only pay for resources used. This cost-efficiency is valuable for agencies or countries with limited budgets.	Cost-efficiency makes cloud adoption viable for smaller states or organizations that seek to enhance security capabilities without major investments in infrastructure.
Collaboration and real-time information-sharing[44]	Cloud computing facilitates secure, real-time information-sharing across borders, which is critical for international alliances and partnerships.	The cloud enables allies to partners to joint conduct military or humanitarian operations by providing a shared digital space for data access and coordination.
Enhanced data analytics and intelligence processing[45]	Cloud platforms provide powerful data-processing capabilities that allow for advanced analytics, machine learning and AI applications. These tools can transform large volumes of raw data into actionable intelligence.	This capability enables faster and more accurate intelligence analysis, improving situational awareness and supporting proactive threat detection.

42 Beckie Orszula, "The Benefits of Disaster Recovery in the Cloud", InterVision, 19 July 2024, https://intervision.com/blog-benefits-of-disaster-recovery.

43 Manal Zarik, "Optimizing the Cloud for Cost-Efficiency and Performance", Leyton, 20 February 2024, https://leyton.com/ca/insights/articles/optimizing-the-cloud-for-cost-efficiency-and-performance.

44 Tim Wanger, "What is Real-Time Data Sharing?", Vendia, 2 May 2022, https://www.vendia.com/blog/what-is-real-time-data-sharing.

45 Ironhack, "The Role of Cloud Computing in Enhancing Data Analysis", 14 July 2023, https://www.ironhack.com/gb/blog/the-role-of-cloud-computing-in-data-analysis.

Table 3. Overview of risks of cloud computing

ISSUE	DESCRIPTION	IMPLICATIONS
Data sovereignty and jurisdictional challenges[46]	Data stored in a data centre in a different country is subject to the jurisdiction of the host country. While redundancies and backups of data across data centres in different countries may somewhat offset the risk of interferences by the country hosting the cloud infrastructure, the issue of jurisdiction remains one to be further explored.	For government agencies, especially defence and intelligence agencies, cloud-based data storage outside the home jurisdiction may introduce a risk of foreign surveillance or limitations on data access. This could impair national security operations, create vulnerabilities in data protection, and raise compliance issues when dealing with sensitive or classified information.
Cybersecurity threats and attack surface expansion[47]	Cloud environments, especially public clouds, increase the attack surface. This makes them attractive targets for cyberattacks, including data breaches, distributed denial of service (DDoS) attacks and ransomware. While leading cloud service providers invest heavily in cybersecurity, the complexity of multitenant environments can introduce vulnerabilities, and any breach could affect numerous clients at once.	For critical infrastructure (e.g., energy, water and healthcare systems) that rely on cloud computing, cyberattacks could disrupt essential services, with wide-ranging impacts on public safety and national stability. Additionally, if military or intelligence data were compromised, it could lead to information exposure, weaken defence postures and erode trust among states cooperating on security.
Vendor lock-in and dependency on major providers[48]	Organizations may become dependent on a small number of dominant CSPs, leading to "vendor lock-in". Some CSPs have already taken steps to mitigate this risk in a deliberate effort to enhance transparency for the customers.[49] However, transitioning to an alternative CSP or returning to on-premises systems could be costly and complex.	For governments and international organizations, reliance on a few CSPs may limit operational flexibility and create vulnerabilities. If a vendor experiences technical problems, service interruptions or even political pressure, this could have an impact on a country's ability to access its own data or maintain control over its operations. Additionally, concentration of cloud infrastructure among a few providers could be exploited by adversaries to disrupt critical systems through targeted attacks on these providers.
Interoperability and international standards[50]	A lot of effort has been made in recent years to develop standards for interoperability and portability[51] However, existing literature suggests that more needs to be done to both widen the adoption of these standards and develop additional ones to cover other aspects pertaining to cloud computing.[52]	For international security, inconsistent use or fragmentation of standards can hinder collaboration among allied states. This could limit the ability to share real-time intelligence, coordinate defence strategies or conduct joint humanitarian missions. Such fragmentation could reduce the effectiveness of coalition responses to global threats and create gaps in the collective defence against cyberattacks.

1.6. What role does cloud computing play in the development and deployment of AI applications?

In the light of the increased interest of the policymaking community in issues pertaining to AI, it is important to unpack the symbiotic relationship that exists between AI and cloud computing.

Cloud computing significantly accelerates AI development, supports the deployment of AI at scale and provides the infrastructure necessary for continuous model improvement. However, it also introduces security, compliance and geopolitical challenges that must be managed to safely integrate AI into international security frameworks.

Selected benefits

Some of the most recognizable benefits of cloud computing for AI include:

- **Enhancing data storage and management**: AI systems rely heavily on vast amounts of data to learn patterns and make predictions.[53] Cloud computing provides secure, scalable storage solutions for the large data sets that AI applications require, supporting both structured and unstructured data formats. Cloud storage solutions (e.g., data lakes) facilitate data ingestion, processing and transformation, which are all critical for feeding AI models with high-quality, diverse data.

---

46 Alex Matthew, "Cloud Data Sovereignty Governance and Risk Implications of Cross-Border Cloud Storage", ISACA, 18 November 2024, https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage; Filippo Gualtiero Blancato, "The Cloud Sovereignty Nexus: How the European Union Seeks to Reverse Strategic Dependencies in its Digital Ecosystem", *Policy & Internet*, vol. 16, no. 6 (2024), https://doi.org/10.1002/poi3.358.

47 David Puzas, "12 Cloud Security Issues: Risks, Threats and Challenges", Crowdstrike, 1 April 2024, https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-security-risks; Alex Delamotte, "The State of Cloud Ransomware in 2024", SentinelOne. 14 November 2024, https://www.sentinelone.com/blog/the-state-of-cloud-ransomware-in-2024; Microsoft Threat Intelligence, "Storm-0501: Ransomware Attacks Expanding to Hybrid Cloud Environments", 26 September 2024, https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments.

48 Justice Opara-Martins, Reza Sahandi and Feng Tian, "Critical Analysis of Vendor Lock-in and Its Impact on Cloud Computing Migration: A Business Perspective", *Journal of Cloud Computing*, vol. 5, no. 4 (2016), https://doi.org/10.1186/s13677-016-0054-z.

49 See, for example, Microsoft's European Cloud Principles: Microsoft, "Microsoft adopts European Cloud Principles", 6 August 2022, https://blogs.microsoft.com/on-the-issues/2022/08/06/microsoft-adopts-european-cloud-principles.

50 Archana Venkatraman, "Lack of Cloud Standards and Interoperability Hinders Cloud Adoption", *Computer Weekly*, 1 August 2012, https://www.computerweekly.com/news/2240160652/Lack-of-cloud-standards-and-interoperability-hinders-cloud-adoption; Ariel Levite and Gaurav Kalwani, *Cloud Governance Challenges: A Survey of Policy and Regulatory Issues* (Washington, DC: Carnegie Endowment for International Peace, 2020), https://carnegieendowment.org/research/2020/11/cloud-governance-challenges-a-survey-of-policy-and-regulatory-issues; John Pendleton, Ariel Levite and Bob Kolasky, *Cloud Reassurance: A Framework To Enhance Resilience And Trust* (Washington, DC: Carnegie Endowment for International Peace, 2024), https://carnegieendowment.org/2024/01/18/cloud-reassurance-framework-to-enhance-resilience-and-trust-pub-91394; Marek Moravcik, Pavel Segec and Martin Kontsek, "Overview of Cloud Computing Standards", 16th IEEE International Conference on Emerging eLearning Technologies and Applications, 2018, https://doi.org/10.1109/ICETA.2018.8572237.

51 See, for example, ISO, "Information Technology – Cloud Computing – Interoperability and Portability", ISO/IEC 19941:2017, 2017, https://www.iso.org/standard/66639.html.

52 See, for example, Lars Herrmann, "Taking a Stand Against Container Fragmentation . . . with Standards", Red Hat, 6 May 2015, https://www.redhat.com/en/blog/taking-stand-against-container-fragmentationwith-standards.

53 Nancy Khandelwal, "Why Data Matters in the AI Revolution", In Time Tec, 25 September 2024, https://blog.intimetec.com/why-data-matters-in-the-ai-revolution.

- **Enabling scalability to manage varying AI workloads**: AI applications, especially those involving deep learning and large language models, require significant computational resources to train, process and refine algorithms. Cloud computing provides scalable resources on demand, allowing organizations to run AI workloads without the need to invest in costly, high-performance hardware.[54] For example, training an AI model on millions of data points requires extensive computational power, which the cloud can provide flexibly. Organizations can scale up resources during training phases and scale down after deployment, thereby optimizing costs and resource usage.
- **Providing access to high-performance computing and specialized hardware**: In addition, modern AI algorithms often rely on specialized hardware, such as graphics processing units (GPUs) and tensor processing units (TPUs), which are designed to handle large-scale data-processing tasks efficiently.[55] These devices are expensive to own and maintain, making cloud service providers an attractive alternative. Leading CSPs offer access to these high-performance resources, enabling faster training and deployment of AI models. By using cloud-based infrastructure, developers can access the latest hardware without needing dedicated on-premises set-ups, thus opening up faster and cheaper ways to experiment and to test new models.
- **Democratizing AI development**: Cloud platforms have democratized access to advanced AI tools, making it possible for smaller organizations and individuals to develop AI applications without extensive infrastructure and allowing better collaboration among AI researchers.[56] Major CSPs offer pre-built AI services (e.g., image recognition, language translation, sentiment analysis and speech-to-text) that developers can incorporate into applications without building AI models from scratch. By offering these ready-to-use application programming interfaces (APIs) and AI services, CSPs enable organizations and individuals to integrate AI capabilities with minimal expertise, speeding up development timelines and reducing costs.
- **Enhancing AI security and compliance**: AI models often process sensitive information, making data security and compliance essential considerations.[57] In order to safeguard data used in AI applications, cloud platforms invest heavily in advanced security measures, such as encryption, access controls and compliance certifications – for example, the European Union's General Data Protection Regulation (GDPR), the United States' Health Insurance Portability and Accountability Act and International Organization for Standardization (ISO) standards. Additionally, CSPs offer tools for monitoring and auditing data usage, which helps ensure that AI applications comply with regulations.

---

54 Paul Estrach, "Scalability in Cloud Computing: A Deep Dive", Mega, 18 August 2023, https://www.mega.com/blog/what-is-scalability-in-cloud-computing.

55 Tunmise Adewale, "Speeding Up AI: How Specialized Hardware is Powering Next-Gen Intelligence", Stanford University, November 2024, https://www.researchgate.net/publication/385855445_Speeding_Up_AI_How_Specialized_Hardware_is_Powering_Next-Gen_Intelligence.

56 Alice Gomstyn and Alexandra Jonker, "Democratizing AI: What Does It Mean and How Does It Work?", IBM, 5 November 2024, https://www.ibm.com/think/insights/democratizing-ai.

57 Max Wolf, "AI Data Security: Insights and Best Practices", Veeam, 20 August 2024, https://www.veeam.com/blog/ai-data-security.html; Arthur, "Safeguarding Data Protection and Compliance when utilizing AI", Hey Data, 14 May 2024, https://heydata.eu/en/magazine/safeguarding-data-protection-and-compliance-when-utilizing-ai-.

- **Cost-effectiveness for AI development**: Developing AI models on-premises can be prohibitively expensive, especially for organizations with limited budgets. Cloud computing's pay-as-you-go pricing model allows companies and organizations to develop and deploy AI applications without significant upfront investment. Instead of purchasing costly hardware, organizations can allocate resources based on their immediate needs, optimizing costs for different stages of AI development.

Key implications for international security

The role of cloud computing in AI development and deployment has important implications for international security that build on the general list above (see tables 2 and 3). For example, while cloud computing democratizes AI access, it can also make AI capabilities more accessible to malicious actors, who might use AI for information operations, cyberattacks or other malicious purposes (described further in section 2.2).

In addition, AI models trained on sensitive or personal data present challenges related to data sovereignty and cross-border regulations. For international security, hosting AI models on cloud platforms with data centres across different jurisdictions may complicate compliance with national security regulations and privacy laws (see section 2.1), which would also hinder collaboration and cooperation efforts.

Part 2. Governance primer

Recent years have not only seen accelerating technological innovations across fields and sectors, but a growing appreciation of the need for governance frameworks to ensure that the benefits of emerging technologies are maximized and that any associated risks are reduced.[58] This trend has been accelerated by the dual-use nature of technologies, which adds an international security, geopolitical and global layer to their governance. This is visible in, for example, the push for a global approach to governance of artificial intelligence in both civilian and military domains.[59]

While policy attention has begun to be directed towards various aspects of cloud computing, a cohesive, global discussion of cloud computing governance has yet to emerge. However, as a critical enabling technology and important underlying layer of the global digital economy with implications for international peace and security, the governance of cloud computing should receive attention from the international peace and security community.

Hence, this part of the report provides a springboard for this discussion. It first highlights some of the key existing challenges with respect to cloud computing governance that are relevant in the context of international security. It then explores some of the implications for arms control.

2.1. What are the challenges of governing cloud computing?

Cloud computing, with its vast underlying infrastructure and various technological components, does not exist in a regulatory vacuum – it is already subject to a complex, overlapping and layered regulatory constellation.[60] As a "system of systems" of technologies, comprising a multitude of services across sectors and national borders, the cloud computing governance landscape comprises a varied combination of national legislation and regulations, international agreements, and national and international initiatives and standards. This has resulted in a relatively fragmented governance landscape.[61] This is a consequence of challenges stemming from factors inherent to the technology – and business model – itself, as well as broader factors linked to the geopolitical and international security context with which cloud computing intersects. This highlights the need to explore whether greater regulatory alignment in cloud computing governance is needed in order to maximize the effective use of the technology.[62]

---

58 General Assembly, "The Pact for the Future", Resolution 79/1, 22 September 2024, https://www.undocs.org/A/RES/79/1.

59 High-Level Advisory Body on Artificial Intelligence, *Governing AI for Humanity* (New York: United Nations, 2024), https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf; Yasmin Afina, *The Global Kaleidoscope of Military AI Governance: Decoding the 2024 Regional Consultations on Responsible AI in the Military Domain* (Geneva: UNIDIR, 2024), https://unidir.org/wp-content/uploads/2024/09/UNIDIR_The_Global_Kaleidoscope_of_Military_AI_Governance.pdf.

60 Pendleton, Levite and Kolasky, *Cloud Reassurance*.

61 Levite and Kalwani, *Cloud Governance Challenges*.

62 Some potential risks linked to growing governance fragmentation could include added complexity to operational cyberdefence and the ability to defend against growing cyberthreats; difficulty in implementing consistent security measures across different jurisdictions; or the complexity of conducting time-sensitive incident response activities.

While not exhaustive, the most salient governance challenges include:

- Complexity
- Geographical and market concentration
- Intersection with other technology governance efforts
- Digital sovereignty
- Increased use in the military domain

There is a role for regulation in improving cloud computing governance and resilience. However, to maximize the regulations' effectiveness, it would be important to reduce complexity and better align regulations and laws governing this technology. To foster greater harmonization for a more global approach to cloud computing governance that better guards against potential risks to international security this section briefly expands on each of the above governance challenges (with an overview in Table 4). It shows how each contributes to rendering the governance of cloud computing particularly difficult and fragmented.

Complexity

Experts have referred to cloud service providers as "magnificent engines of complexity".[63] The cloud comprises an intricate network of technologies (both hardware and software), services and actors operating on a global scale across sectors.[64] This has practical implications for governance. Principally, it entails that the system is particularly complex for regulators and would-be governing bodies to fully understand, and in turn to design comprehensive governance frameworks for.[65] As a system of systems of technologies, cloud computing is inherently opaque; clearly understanding the relationships between its various elements, clearly identifying risk nodes, and effectively applying regulatory tools to stem these risks is a Herculean task.[66]

Hence, in place of cohesive system-wide frameworks, the complexity of the cloud has been a key driver behind the fragmentation of its governance landscape, resulting in an equally complex patchwork of policies, legislation and standards in different sectors, industries and countries. The cloud is now subject to a host of national regulations, legislation and policies and national and international certification schemes and technical standards that apply to both CSPs and costumers.[67] These can be sector specific (e.g., regulating use of cloud services in the healthcare sector) or aspect specific (e.g., data-management policies, cybersecurity requirements). Moreover, the maturity or even presence of regulations pertaining to cloud services varies drastically across sectors and jurisdictions.[68] The complexity of the cloud further means that a multitude of stakeholders – from various government agencies, international organizations and bodies, and industry actors – with overlapping or divergent interests, goals and priorities are involved in governance or can claim regulatory oversight over certain aspects of cloud computing.[69]

---

63 Trey Herr, *Four Myths About the Cloud: The Geopolitics of Cloud Computing* (Washington, DC: Atlantic Council, 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/09/CLOUD-MYTHS-REPORT.pdf.

64 Zuo et al., *Critical Infrastructure and the Cloud*.

65 Ibid.

66 Ibid.

67 Maria Hamin, Trey Herr and Marc Rogers, "Cloud Un-Cover: CSRB Tells It Like It Is But What Comes Next Is on Us", Lawfare, 28 May 2024, https://www.lawfaremedia.org/article/cloud-un-cover-csrb-tells-it-like-it-is-but-what-comes-next-is-on-us; Levite and Kalwani, *Cloud Governance Challenges*.

68 Ibid.

69 Levite and Kalwani, *Cloud Governance Challenges*.

For instance, in the European Union alone, the AI Act, the Cyber Resilience Act, the Data Act, the Digital Operational Resilience Act (DORA), the GDPR and the Network and Information Security (NIS) Directives as well as the incoming Cloud Certification Scheme all have implications for CSPs along with national requirements of its 27 member states.[70] Similarly, in the United States, no single authority has a clear mandate to set requirements for the cloud ecosystem.[71] The FedRAMP programme and diverse guidance and standards from the National Institute of Standards and Technology (NIST) provide CSPs with various security requirements, while sector-specific regulators seek their own requirements to ensure service continuity.[72] Internationally, a host of technical standards by the ISO, the Institute of Electrical and Electronics Engineers (IEEE) and the Cloud Security Alliance as well as data-localization laws add a further layer of regulatory complexity.[73]

By increasing the difficulty of compliance, regulatory inconsistency and fragmentation can adversely affect cloud security.[74] As CSPs and their customers navigate this landscape, the risk of inconsistent application of the dizzying number of standards and regulations is high. Notably, as a by-product, experts note that this entails that only the largest companies can bear the costs of compliance, which further solidifies market concentration.[75] The complexity of cloud computing is not likely to reduce, and a comprehensive catch-all governance framework for cloud computing writ large is equally unlikely and potentially undesirable. Successful governance of cloud computing, therefore, partially rests on the ability to manage this regulatory complexity, to harmonize governance frameworks and regulations, and to pursue greater international and national coordination and interoperability in order to minimize gaps and contradictions among frameworks. Conversely, continuous fragmentation could come at the cost of cloud security, safety and resilience.[76]

Geographical and market concentration

Despite its global, networked and complex nature, cloud computing exhibits extremely high levels of market concentration.[77] Even though many CSPs act as global utility providers by distributing their service over large geographic areas, this market and geographical concentration carries with it important governance implications.

---

70 For more information on individual European Union policies and regulations pertaining to cyberspace, see UNIDIR, "European Union (EU)", Cyber Policy Portal, November 2023, https://cyberpolicyportal.org/organizations/european-union-eu.

71 Levite and Kalwani, *Cloud Governance Challenges*.

72 Ibid.

73 ISO, "Cloud Computing", n.d., https://www.iso.org/ics/35.210/x; IEEE Computer Society, "Standards in Cloud Computing", n.d., https://tc.computer.org/tccld/standards; Cloud Security Alliance, "Standards", n.d., https://cloudsecurityalliance.org/research/topics/standards.

74 Hamin, Herr and Rogers, "Cloud Un-Cover".

75 UNIDIR, "Technology and Security Seminar on Cloud Computing: Exploring Implications for International Security and Governance", 30 September 2024, https://unidir.org/event/technology-and-security-seminar-on-cloud-computing-exploring-implications-for-international-security-and-governance.

76 Hamin, Herr and Rogers, "Cloud Un-Cover"; Levite and Kalwani, *Cloud Governance Challenges*.

77 The 10 largest CSPs are concentrated in three countries, and the top 3 capture 65% of the global market. For more information, see Zuo et al., *Critical Infrastructure and the Cloud*; Mary Zhang, "Top 10 Cloud Service Providers Globally in 2024", Dgtl Infra, 18 April 2024, https://dgtlinfra.com/top-cloud-service-providers.

First, market concentration provides large CSPs with strong influence over regulatory and governance discussions.[78] Like much recent technological innovation, cloud computing is an industry-led effort, with research and innovation taking place in the private sector. Therefore, the design and security choices of a handful of industry players effectively become the realities of the technology and, more broadly, the global digital economy.[79] In this respect, they exert influence on the trajectory of cloud computing.

Second, the geographic provenance of CSPs has had – as discussed further below – a knock-on effect on the governance of cloud computing by contributing to the importance of digital sovereignty.

Third, the size of the largest CSPs has created a knowledge imbalance between the operators of the cloud and regulatory authorities. Coupled with the above-mentioned complexity, this has created a high level of opacity, whereby regulators have limited visibility into the practices – both business and security – of CSPs.[80] This is further exacerbated by the fact that the very management of complexity can be at the heart of a CSP's competitive advantage, and therefore a closely guarded secret.[81]

Intersection with other technology governance efforts

Further complexifying the picture is the reality that the governance of any given technology does not happen in a silo, independent of other technologies and their related governance discussions. Predictably, 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. This not only means that devising a cohesive, focused effort around cloud computing is difficult to achieve, 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 other technologies.[82] The deep embedding of cloud computing within the broader AI governance discussion is of particular note. Indeed, an emergent discussion in AI governance frames cloud computing as a tool in the AI governance toolbox. In essence, these proposals seek to govern certain aspects of AI – mainly access to computing power and microchips– *through* the cloud.[83]

78 Herr, *Four Myths About the Cloud*.

79 Tim Mauer and Garrett Hinck, *Cloud Security: A Primer for Policy Makers* (Washington, DC: Carnegie Endowment for International Peace, 2020), https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.

80 Mauer and Hinck, *Cloud Security*; Hamin, Herr and Rogers, "Cloud Un-Cover".

81 Zuo et al., *Critical Infrastructure and the Cloud*.

82 Tim Fist and Paul Scharre, "The Cloud Can Solve America's AI Problem", *Foreign Policy*, 7 October 2023, https://foreignpolicy.com/2023/10/07/cloud-computing-artificial-intelligence-chips-sanctions-us-china.

83 Lennart Heim et al., "Governing Through the Cloud: The Intermediary Role of Compute Providers in AI Regulations", University of Oxford, 2024, https://doi.org/10.48550/arXiv.2403.08501.

Proponents highlight access to computing power as a key bottleneck where regulatory control can be exerted. This is due to the fact that cloud computing is (a) emerging as the primary way through which to access the computational resources to develop, train and deploy advanced AI systems, (b) because the compute power needed to train an algorithm is a good indication of its level of sophistication, and (c) because it is a visible, quantifiable, concentrated and tangible.[84] In contrast to a more global approach, this focused approach – in this case utilizing governance of cloud computing to achieve AI governance goals – could, however, potentially exacerbate power imbalances with regards to AI governance. Indeed, this approach would, for example, see more regulatory power conferred on the few countries that physically host the most advanced computing power infrastructure, mainly concentrated in the so-called Global North.[85]

Hence, the shape of the cloud computing landscape is also affected by discussions, needs, goals and actions taken in governance efforts in adjacent fields. Cloud computing's cross-sectoral, multi-technology, pervasive and global nature challenges traditional, siloed governance approaches. Convergence between technologies (e.g., with advances in quantum computing) will further entrench the need for agile governance approaches. In this context, increasing cross-fertilization with other governance efforts is likely to be a critical way in which to maximize alignment between the goals and actions across efforts.

Digital sovereignty

Discussions surrounding the governance of cloud computing are inextricably linked to the concept of "digital sovereignty". This can be broadly defined as the objective by states of "maintaining or achieving an acceptable level of autonomy or independence in the use of digital technologies".[86] The centrality of digital sovereignty to cloud computing governance efforts has principally been the result of the geographical concentration of major CSP 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.

At its core, cloud computing is about data: its movement, storage, access, processing, sharing and monetization. It follows, therefore, that cloud computing governance is linked to – and influenced by – both data governance and states' economic, national security and societal concerns around data.[87] Hence, the main legislative reflex that many states have had with respect to cloud computing – with the aim of digital sovereignty – has been to seek to establish sovereignty over their cloud environments through data-localization laws and requirements.[88] This has been done to extend a territory-based logic of "control" and jurisdiction to data.[89] At least 40 states have some form of data-localization (or

---

84 Ibid.

85 Vili Lehdonvirta, Boxi Wu and Zoe Hawkins, "Compute North vs. Compute South: The Uneven Possibilities of Compute based AI Governance Around the Globe", Proceedings of the 7th AAAI/ACM Conference on AI, Ethics and Society, 2024, https://doi.org/10.31235/osf.io/8yp7z.

86 Blancato, "The Cloud Sovereignty Nexus".

87 Herr, *Four Myths About the Cloud*.

88 "Global Data Governance, Part One: Emerging Data Governance Practices", *Foreign Policy*, 13 May 2020, https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map.

89 D. Svantesson, *Data Localisation Trends and Challenges: Considerations for the Review of Privacy Guidelines* OECD Digital Economy Papers no. 305 (Paris: OECD Publishing, 2020), https://doi.org/10.1787/7fbaed62-en.

residency) requirements with various degrees of stringency: these range from requirements that all data be stored, processed and accessed within a confined geographic space to requirements that a copy of data be stored locally, and many other combinations in between.[90] Common justifications for these requirements are related to security and privacy (i.e. increasing cybersecurity and data privacy), economic (i.e. extracting value from data) and geopolitical (i.e. preventing foreign espionage and gaining geopolitical advantage).[91]

Digital sovereignty – and data localization in particular – has had some of the most direct and important impacts on shaping the global cloud computing landscape. Indeed, it has been one of the main forces driving CSPs to build data centres in specific locations, to subcontract to domestic actors, and to develop so-called sovereign clouds or data boundaries, which guarantee the storage, processing and accessing of data within a confined geographical region.[92] In other cases, entire efforts have been directed at building a fully "sovereign" cloud market (e.g., GAIA-X, a European effort to build a "European federated cloud environment" with European-owned providers, infrastructure, technologies and standards), echoing the importance of digital sovereignty.[93]

However, the net effect of data localization is disputed. While serving national security and economic goals, some have argued that these requirements may come at the cost of other cloud governance objectives, such as security, sustainability, or respect for human rights.[94] For example, they might necessitate the construction of more data centres, consolidating the market power of a few incumbent companies, reducing security, or potentially enabling abusive government to access citizen data. Additionally, it has been argued that data-localization requirements are politically motivated, quasi-protectionist measures intended to boost domestic cloud ecosystems, and that they are not effective tools to address cloud computing risks.[95] For example, the current deadlock over the European Union's Cloud Certification Scheme is partially caused by disagreements over proposed requirements intended to boost digital sovereignty.[96]

---

90 Ibid. The exact number of states with data localization laws is subject to debate, with some sources estimating 60–100. For other estimates see David Medine, "Data Localization: A 'Tax' on the Poor", Center for Global Development, Working Paper no. 674, January 2024, https://www.cgdev.org/sites/default/files/data-localization-tax-poor.pdf; Deepak Gupta, "Data Localization is Now a Big Part of Doing Business Globally", Brink, 21 October 2021, https://www.brinknews.com/data-localization-is-now-a-big-part-of-doing-business-globally.

91 Svantesson, *Data Localisation Trends and Challenges*.

92 Blancato, "The Cloud Sovereignty Nexus"; Amazon Web Services, "AWS Plans to Invest €7.8 Billion into the AWS European Sovereign Cloud", 15 May 2024, https://www.aboutamazon.eu/news/aws/aws-plans-to-invest-7-8-billion-into-the-aws-european-sovereign-cloud; Julie Brill, "Microsoft Cloud Enables Customers to Keep All Personal Data within European Data Boundary", Microsoft EU Policy Blog, 11 June 2024, https://blogs.microsoft.com/eupolicy/2024/01/11/microsoft-cloud-european-data-boundary.

93 Mathew Gooding, "Gaia-X: Has Europe's Grand Digital Infrastructure Project Hit the Buffers?", Data Centre Dynamics, 13 May 2024, https://www.datacenterdynamics.com/en/analysis/gaia-x-has-europes-grand-digital-infrastructure-project-hit-the-buffers.

94 Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, Global Economy & Development Working Paper no. 113 (Washington, DC: Brookings, 2018), https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_working-paper.pdf; Pendleton, Levite and Kolasky, *Cloud Reassurance*; Medine, "Data Localization".

95 Blancato, "The Cloud Sovereignty Nexus".

96 Cynthia Kroet, "Decision on Cloud Certification Scheme Delayed to Mid-July", Euronews, 18 June 2024, https://www.euronews.com/next/2024/06/18/decision-on-cloud-certification-scheme-delayed-to-mid-july.

The proliferation of data-localization requirements in the service of digital sovereignty, alongside the spread of cloud computing, highlights the inherent tension between, on the one hand, the need for free flow of data as the very rationale underpinning cloud computing and, on the other, the desires for states to maintain control over the way data is stored, accessed, moved and monetized in their territories. This has elevated cloud governance to an issue of geopolitical proportions subject to global technology competition and has enmeshed it in states' efforts to project regional attitudes towards data governance and privacy, and digital governance more broadly.[97] This has had the net effect of exacerbating the fragmentation of cloud computing governance approaches, creating differing privacy and security requirements and standards across regions.[98] Hence, a key governance goal should be to seek to balance states' legitimate concerns over privacy, espionage and sovereignty with the benefits of a global unimpeded cloud computing environment.

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.

First, there are direct implications arise from the increased use of cloud computing by armed forces to deliver warfighting capabilities. Cloud computing is becoming a key way through which armed forces process, analyse, use and share data, as well as develop and run digital or AI-enabled capabilities (as noted in Sections 1.4 and 1.6).[99] As battlefield success becomes a function of this process, done at speed and at scale, cloud computing becomes a key vector through which to deliver combat power. For this, armed forces principally turn to the same CSPs that manage the commercial cloud, making large private technology firms the key enablers of this process.[100] The growing dependence on a few private entities for the delivery of growingly critical military digital services furthers these companies' influence on military affairs.[101] This also entails that governance discussions surrounding the military use of cloud computing must account for the importance and influence of private technology firms as actors in and of themselves, highlighting the need for novel ways of developing public–private governance models.

---

97 Lewis, "An Overview of Global Cloud Competition".

98 Federico Fabbrini and Edoardo Celeste, "Competing Jurisdictions: Data Privacy Across the Borders", in *Data Privacy and Trust in Cloud Computing*, eds Gerard Theorore Lyn et al. (Cham: Palgrave Macmillan, 2021), https://link.springer.com/book/10.1007/978-3-030-54660-1.

99 Tom Biddle, "U.S. Military Makes First Confirmed OpenAI Purchase for War-Fighting Forces", The Intercept, 25 October 2024, https://theintercept.com/2024/10/25/africom-microsoft-openai-military.

100 Jon Harper, "Pentagon Awards Nearly $1B in JWCC Task Orders", DefenseScoop, 7 August 2024, https://defenscoop.com/2024/08/07/pentagon-awards-nearly-1b-jwcc-task-orders; Esat Dedezade, "Thales and Microsoft Partner to Develop a Unique Defence Cloud Solution", Microsoft, 12 June 2018, https://news.microsoft.com/europe/2018/06/12/thales-and-microsoft-partner-to-develop-a-unique-defence-cloud-solution; Caroline Haskins, "The Hidden Ties Between Google and Amazon's Project Nimbus and Israel's Military", Wired, 15 July 2024, https://www.wired.com/story/amazon-google-project-nimbus-israel-idf; Jack Poulson, "Militaries, Intelligence Agencies, and Law Enforcement Dominate U.S. and U.K. Government Purchasing from U.S. Tech Giants", Tech Inquiry, 2022, https://techinquiry.org/docs/InternationalCloud.pdf.

101 Bruno Maçães, "How Palantir Is Shaping the Future of Warfare", *Time*, 10 July 2023, https://time.com/6293398/palantir-future-of-warfare-ukraine; Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab", *Time*, 8 February 2024, https://time.com/6691662/ai-ukraine-war-palantir.

This could potentially also exacerbate the governance challenge regarding digital sovereignty due to the raising of the sensitivity of the data stored, processed and moved in the cloud. This both reinforces the desire for digital sovereignty in the context of cloud environments, resulting in further fragmentation of cloud computing governance, and potentially makes international cooperation and approaches to cloud governance harder to achieve.[102]

Furthermore, the cross-border nature of cloud computing entails that, in many cases, data is stored across jurisdictions, sometimes in multiple places at once.[103] In the case of military or sensitive government data, this raises unanswered questions in times of conflict. For example, the migration or presence of a belligerent's sensitive data in data centres operated by a CSP in a non-belligerent country – while ensuring continuity of government and critical services – raises questions about the potential targetability of such centres in the non-belligerent, with implications for conflict escalation. Additionally, this also raises concerns with regards to the potential influence exerted by the non-belligerent country or the company on the conflict.[104]

Second, there are governance challenges linked to the provision of digital services by CSPs in times of conflict. While the cloud environments utilized by armed forces or other defence stakeholders may be separated from commercial clouds, this is not the case by default. Even if they are separate, this nonetheless results in the same technology firms providing digital services to armed forces and civilians alike. This potentially raises questions with respect to international humanitarian law.[105] Indeed, some experts have suggested that the presence of private technology firms in hostilities, through the provision of digital services, might raise questions under international humanitarian law about whether their infrastructure and personnel could potentially be considered lawful targets.[106] The unclear division between, on the one hand, services provided for armed forces and their combat goals and, on the other, services provided to civilian populations entails the potential for cascading effects on civilians and civilian infrastructure. Due to this, experts have advocated for a clear separation of public commercial and private clouds from armed forces' use of cloud computing services in order to decouple civilian and military digital infrastructure.[107]

---

102 Reuters, "Italy, Europe Need State-Controlled Cloud Services – Leonardo Chief", 25 October 2023, https://www.reuters.com/world/europe/italy-europe-need-state-controlled-cloud-services-leonardo-chief-2023-10-25.

103 Herr, *Four Myths About the Cloud*.

104 Tara Copp, "Elon Musk's Refusal to have Stalking Support Ukraine Attack in Crimea Raises Questions for Pentagon", Associated Press, 12 September 2023, https://apnews.com/article/spacex-ukraine-starlink-russia-air-force-fde-93d9a69d7dbd1326022ecfdbc53c2.

105 Jonathan Horowitz, "The Business of Battle: The Role of Private Tech in Conflict", Lawfare, 17 September 2024, https://www.lawfaremedia.org/article/the-business-of-battle--the-role-of-private-tech-in-conflict.

106 Jonathan Horowitz, "One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict", *Chicago Journal of International Law*, vol. 24, no. 2 (2024), https://cjil.uchicago.edu/sites/default/files/2024-02/Horowitz_One Click from Conflict.pdf.

107 International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts* (Geneva: ICRC, 2024), https://rcrcconference.org/app/uploads/2024/09/34IC_10.6-IHL-Challenges-Report-EN.pdf; Horowitz, "One Click from Conflict".

Hence, as armed forces seek to benefit from the cost-saving, elasticity and speed provided by cloud computing solutions, they reinforce two major international security trends: the increased meshing of civilian and military technologies and the growing place of technology firms in conflicts. These are recognized governance challenges for dual-use technologies across the board. With cloud computing, however, the impact is amplified due to how fundamental the services provided are, and the implications for civilian infrastructure and services of the increased involvement of CSPs in potential conflict scenarios.[108]

Table 4. Summary of governance challenges and implications for cloud computing governance

GOVERNANCE CHALLENGE	IMPLICATIONS FOR CLOUD COMPUTING GOVERNANCE
Complexity	• 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	• 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	• Overlap with other governance discussions and efforts • Influence of adjacent governance discussions, efforts and actions on cloud computing landscape • Growing need for cross-fertilization of governance efforts across technological fields
Digital sovereignty	• 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	• 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

108 Horowitz, "One Click from Conflict".

2.2. What are the implications of cloud computing for arms control?

Warfare in the 21st century increasingly features digitalized, intangible and dual-use means.[109] This entails that the capabilities that arms control mechanisms seek to constrain growingly share these characteristics.[110] Increasingly, these capabilities are being developed, stored, shared and accessed through the cloud. Moreover, much of the world's digital infrastructure now relies on the functioning and continuity of cloud computing services. This double reality entails that cloud computing interfaces with arms control in two key ways. First, cloud computing and its related infrastructure – as a critical layer of society and the economy and an enabler of digital connectivity and digital innovation – warrants protection.[111] Second, cloud computing – as a means to access and develop disruptive dual-use digital capabilities or otherwise move and access digitally stored information that is subject to arms control provisions – requires oversight.

Hence, two key goals for arms control in the context of cloud computing emerge: protecting the cloud; and developing "digital twins" of arms control concepts for the cloud.[112]

Protecting the cloud

Arms control is not only about weapon systems but also about behaviours and norms. As noted throughout this report, cloud computing failures, either accidental or as the result of adversarial action, could have serious consequences across society. With the increased prevalence of cloud computing in defence contexts, any compromise of cloud services could have serious international security implications. Therefore, as stakes rise along with adoption of cloud computing, 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, cloud computing does not exist in an international normative vacuum. The 11 United Nations Norms of Responsible State Behaviour in Cyberspace outline a set of common expectations for state behaviour. Similarly, consensus exists with respect to the applicability of international law in cyberspace.

In its 2021 report, the General Assembly's Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security states that "Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities."[113] The 2022 report of the Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies repeats this language.[114]

---

109 Amy J. Nelson, "How Emerging Technology is Breaking Arms Control", Lawfare, 24 April 2024, https://www.lawfaremedia.org/article/how-emerging-technology-breaking-arms-control.

110 Ibid.

111 While cloud infrastructure – as a civilian object – is protected by international humanitarian law, it is important to note the ongoing debate over the extent to which civilian cloud data can be treated as a civilian object, and therefore protected. As the cloud requires both to function, this is an important area to be further clarified.

112 In the context of this report, "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.

113 General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, https://undocs.org/A/76/135, paragraph 10.

114 General Assembly, Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/77/275, 8 August 2022, https://undocs.org/A/77/275, paragraph 10.

As laid out above, cloud computing (and its underlying infrastructure) provides both essential services to the public and technical infrastructure essential to the general availability or integrity of the Internet. Therefore, without explicitly mentioning it, this normative framework inherently encompasses the cloud and its related infrastructure as critical information infrastructure. So, the protection of cloud infrastructure starts with the implementation of the commitments under the framework of responsible state behaviour in the use of ICT. However, concerns have been voiced, particularly by industry representatives, over the need to further develop the framework (e.g., with the development of a new norm) to provide stronger and dedicated protection to cloud services.[115]

However, cloud computing is not only a cybersecurity issue and treating it exclusively as such risks resulting in governance blind spots. As a network of physical infrastructure, focus should also be placed on the physical security and integrity of the cloud. Increased military use of cloud computing makes it a critical risk node, a potentially alluring target and, in some cases, a potentially legitimate one under international humanitarian law. However, due to the above-mentioned entwinement between civilian and miliary cloud infrastructure, even legitimate targeting of an armed force's digital infrastructure could have cascading effects across civilian infrastructure. To avoid this, 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.[116]

Developing "digital twins" of arms control concepts: the case of export controls

Traditional arms control concepts do not transfer very well into the realities of cloud computing. The former are concerned with territoriality, state control, physical verification capabilities, and restriction on the movement and access to information, technologies and capabilities. The latter, in contrast, is predicated on the need for flexible, quick and dynamic transfer of data across locations and borders. To date, little discussion and work has been undertaken to unravel this inherent tension.

However, cloud computing could potentially act as a multiplier of proliferation risk, by multiplying the vectors through which disruptive digital dual-use capabilities, controlled software or technical data can be accessed, stored, shared and developed, due either to controlled data or software being stored in or routed through a foreign state, or it being accessed by foreign nationals.[117] Arms control mechanisms should therefore seek to confer the international community with the capabilities to verify and control by whom, and for what, cloud computing is being used. In this context, however, the application "as is" of arms control tools to govern new technological realities is likely to continue to be of limited utility. The ability of the international community 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.

---

115 Microsoft, *Microsoft Digital Defense Report 2024* (Redmond, WA: Microsoft, 2024), https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

116 Pendleton, Levite and Kolasky, *Cloud Reassurance*.

117 Mark Bromley and Giovanna Maletta, *The Challenge of Software and Technology Transfer to Non-Proliferation Efforts: Implementing and Complying with Export Controls* (Stockholm: Stockholm International Peace Research Institute, 2018), https://www.sipri.org/sites/default/files/2018-04/sipri1804_itt_software_bromley_et_al.pdf.

For example, cloud computing fundamentally challenges export controls, an important tool in the arms control toolbox.[118] Export controls have been the principal focus of discussions surrounding how arms control can be applied in the context of cloud computing.[119] States have attempted to superimpose the traditional model of export controls to the realities of cloud computing, leading to divergences and fragmentation in this space as well. However, the complexities and realities of the cloud have led to divergences across states at a fundamental level, such as *what* constitutes an export in the context of cloud computing or even *when* an export is deemed to have taken place.[120] While discussions have taken place, principally in the United States or within the European Union, there has been little to no international coordination.[121] Cloud computing further challenges key elements of export control: verification, compliance and enforcement capabilities.[122] Indeed, it complexifies the ability for regulators to exert oversight and control over these transfers due to the complexity of the cloud, the dynamic flow of data across borders and the opacity of the process.[123]

Furthermore, proliferation risks with respect to cloud computing are not only limited to the export and transfer of controlled technical information on conventional capabilities or transfer of software, but also the access to the computational power and infrastructure needed to develop capabilities, especially AI-enabled ones. By enabling access to computational resources at a distance, cloud computing lowers the bar of entry for the development of potentially disruptive digital capabilities. For example, experts have noted the potential ability for states – as well as non-state actors – subject to sanctions or arms embargoes to train AI capabilities through the cloud, thereby forgoing the need for specialized materials and data centres and circumventing the international restrictions.[124] In fact, remote access to computing power entails a reduction in the need to build infrastructure or physically assemble capabilities and therefore acquire and move objects and hardware from point to point. This lack of physicality removes a critical control point traditionally used by the international community and challenges the ability of export controls to manage access to certain capabilities. This necessitates the development of novel ways of operationalizing "control" in the context of cloud computing, by understanding what concepts and tools can have greater effect.

---

118 Ibid.

119 Ibid.

120 Ibid.

121 UNIDIR, "Technology and Security Seminar on Cloud Computing".

122 Ibid.

123 Ibid; Guangyu Qiao-Franco and Mahmoud Javadi, "Symposium on Military AI and the Law of Armed Conflict: Navigating the Governance of Dual-Use Artificial Intelligence Technologies in Times of Geopolitical Rivalries", OpinioJuris, 4 March 2024, https://opiniojuris.org/2024/04/03/symposium-on-military-ai-and-the-law-of-armed-conflict-navigating-the-governance-of-dual-use-artificial-intelligence-technologies-in-times-of-geopolitical-rivalries.

124 Hyuk Kim, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications", 38 North, 23 January 2024, https://www.38north.org/2024/01/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications; US Department of Homeland Security, "Addressing Risks from Non-State Actors' Use of Commercially Available Technologies", 2023, https://www.dhs.gov/sites/default/files/2023-09/07. Addressing Risks of COTS Tech_508_0.pdf.

Recent efforts in the United States precisely seek to give the US Government greater insight into who is utilizing United States-based computational resources. Indeed, the US Department of Commerce's Bureau of Industry and Security (BIS) is currently developing "Know Your Customer" rules applicable to providers of infrastructure as a service (IaaS), which would require United States-based providers to collect and disclose information on foreign customers using IaaS to train large AI models.[125] However, industry comments on the proposed rules show the difficulty in applying rules that effectively differentiate legitimate use of cloud services for civilian technologies from use and access for national security purposes.[126]

Hence, the ability to effectively apply access controls and ensure end-user verification in a cloud computing environment will be central to states' abilities to manage the proliferation of military AI capabilities through the cloud. To this end, licensing regimes for computing providers and users are a potential area of research to be further explored.[127] Indeed, they are becoming a popular concept in the context of the AI governance.[128] In the context of cloud computing, licensing regimes could be explored as a tool to vet and monitor access to large amounts of computing power through the cloud. Cloud computing providers could require licences to be able to provide their services for AI training above a certain threshold, while also being subject to reporting requirements.[129] Similarly, issuing licences to users could also impose requirements at various stages of the AI development life cycle.[130] Future areas of research should thus focus on developing novel ways of thinking, and understanding what new tools can better serve the needs of 21st century arms control.

---

125 Kevin Allison and Paul Tiolo, "Know-Your-Customer Is Coming for the Cloud – The Stakes are High", Lawfare, 29 April 2024, https://www.lawfaremedia.org/article/know-your-customer-is-coming-for-the-cloud-the-stakes-are-high.

126 Ian Cohen, "BIS Asked to Hold off on Cloud Export Controls, Clarify Chip Rules", *Export Compliance Daily*, 5 February 2024, https://exportcompliancedaily.com/article/2024/02/05/bis-asked-to-hold-off-on-cloud-export-controls-clarify-chip-rules-2402020050.

127 Falak Ayman Medina, "Malaysia Imposes Licensing Requirements for Cloud Service Providers", ASEAN Briefing, 18 January 2022, https://www.aseanbriefing.com/news/malaysia-imposes-licensing-requirements-for-cloud-service-providers.

128 Gregory Smith, "Licensing Frontier AI Development: Legal Considerations and Best Practices", Lawfare, 3 January 2024, https://www.lawfaremedia.org/article/licensing-frontier-ai-development-legal-considerations-and-best-practices.

129 Microsoft, *Governing AI: A Blueprint for the Future* (Redmond, WA: Microsoft, 2023), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

130 Smith, "Licensing Frontier AI Development".

Conclusion

Cloud computing is an important enabling technology that has unlocked unprecedented levels of connectivity and technological innovation. In so doing, it has become pervasive across society, embedding itself across industries and sectors. Cloud computing confers enormous benefits on adopters by providing scalability, flexibility, resource optimization and cost-efficiency, real-time data processing, as well as increased cyber resilience. Cloud computing is further becoming a key element of the "AI boom", by providing access to the infrastructure and computing power necessary to accelerate the development of artificial intelligence and enable its deployment at scale.

In this context, sectors intersecting with international security are increasingly turning to cloud computing solutions to reap its benefits. In the military domain, cloud computing facilitates, for example, C4ISR, cybersecurity operations, logistics and supply chain management, as well as the development and deployment of AI-enabled capabilities. Critical infrastructure sectors as well as humanitarian and disaster-response sectors similarly benefit from cloud computing's unique characteristics. However, the pervasiveness of, and growing societal dependence on, cloud computing also entails a multitude of risks, with widespread implications for international security.

A fragmented and inconsistent global governance landscape has arisen from the complexity of the cloud, its market and geographical concentration, its intersection with broader technology governance, the centrality of digital sovereignty to the discussions, and its use in the military domain. 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 the 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 reduce the ability of the international community to reap the benefits of cloud computing while addressing its risks.

Importantly, a more in-depth understanding and exploration of the impact on cloud computing on arms control is necessary, lest the cloud's unique characteristics be used to further proliferate disruptive dual-use technologies. This will require a multilateral discussion that focuses on the protection of the cloud, as well as the development of the "digital twins" of various arms control tools adapted to the context of cloud computing. Going forward, this endeavour should not be limited to only cloud computing, as novel technologies will continue to strain the effectiveness of the traditional arms control toolbox.

In the context of multilateral discussion on international ICT security – that is, the current OEWG and the future mechanism currently being negotiated within the OEWG that should be established from 2026 – states should deepen discussion on cloud computing. This should include both an analysis of its unique challenges – and the extent to which the existing normative framework is able to address them – and an analysis of its unique opportunities to help states with the implementation of existing commitments and to boost national cyber resilience.

Given the key role played by cloud service providers, it would be important – and highly recommended – that a geographically representative group of industry players active in this domain is meaningfully involved in such discussions. The same applies for representatives of academia, civil society and the technical community, including security researchers and incident responders. The complexity of the technology and its increased relevance within the ICT environment requires a true multi-stakeholder approach to discuss, design and implement appropriate policy responses.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG