Gobernanza de la computación en la nube

Una reseña de investigación

Federico Mantellassi y Giacomo Persi Paoli

Acerca de esta reseña

Esta reseña de investigación es una versión resumida del informe completo, *Cloud Computing and International Security: Risks, Opportunities and Governance Challenges*, publicado por el Programa de Seguridad y Tecnología del UNIDIR. El informe completo se divide en dos partes: una introducción a la tecnología que ofrece una visión general de las principales aplicaciones de la computación en la nube pertinentes para la seguridad internacional, junto con los riesgos y oportunidades asociados; y una introducción a la gobernanza que analiza los retos a los que se enfrenta la gobernanza de la computación en la nube y sus implicaciones para el control del armamento.

Esta reseña de investigación resume los elementos clave del informe completo, centrándose más en la parte de la gobernanza. Está estructurada en cuatro secciones. La 1.ª sección ofrece un breve resumen de la tecnología. La 2.ª presenta los principales retos de la gobernanza vinculados a la computación en la nube en el contexto de la seguridad internacional y sus implicaciones. La 3.ª sección expone las implicaciones de la computación en la nube para el control de armamento. Y la 4.ª y última sección expone las principales conclusiones del informe completo.

Esta reseña no detalla todo el análisis ni presenta la investigación completa. Para un análisis más detallado de los riesgos y oportunidades para la seguridad internacional de la computación en la nube, su intersección con la inteligencia artificial y un análisis completo de los retos de gobernanza y las implicaciones del control de armas, el lector deberá consultar el informe completo.

Sobre los autores

Federico Mantellassi es investigador del Programa de Seguridad y Tecnología del UNIDIR.

Dr. Giacomo Persi Paoli es responsable del Programa de Seguridad y Tecnología del UNIDIR.

Citación

Federico Mantellassi y Giacomo Persi Paoli, *Gobernanza de la computación en la nube: una reseña de investigación (Ginebra: UNIDIR, 2024).*

1. ¿Qué es la computación en la nube?

La computación en la nube es una tecnología que proporciona a personas y organizaciones acceso bajo demanda a un conjunto compartido de recursos informáticos configurables —como servidores, almacenamiento, aplicaciones y servicios— que pueden ofrecerse y difundirse rápidamente a través de internet[1]. La computación en la nube es un "sistema de sistemas" cuyos elementos básicos pueden desplegarse en diversas configuraciones, con servicios prestados según distintos modelos.

Estos **elementos básicos** incluyen la virtualización, el autoservicio bajo demanda, el amplio acceso a la red, agrupación de recursos, la elasticidad rápida y el servicio medido. Los **modelos de despliegue** son los entornos específicos y las formas en que los servicios en la nube se ponen a disposición de los usuarios. Determinan cómo se asignan los recursos, quién tiene acceso a ellos y cómo se gestiona y a quien pertenece la infraestructura de la nube. Los **modelos de servicio** indican el tipo de servicio que se presta a los usuarios. La figura 1 muestra los componentes clave, el despliegue y los modelos de servicio de la computación en la nube. El Cuadro 1 ofrece una visión general de las principales diferencias entre la computación en la nube y la computación tradicional.

A diferencia de la infraestructura tradicional *in situ* de tecnologías de la información (TI), las arquitecturas basadas en la nube no requieren que las organizaciones posean, mantengan o dediquen recursos como servidores, sistemas de almacenamiento, equipos de red o, incluso, aplicaciones especializadas[2]. En su lugar, estos recursos los proporciona un proveedor de servicios en la nube (CSP) externo, que gestiona la infraestructura remota subyacente, lo que permite a los usuarios centrarse en el despliegue de aplicaciones y la gestión de datos. La computación en la nube es un componente esencial de la infraestructura informática moderna, gracias al cual es posible gran parte de la conectividad global y la innovación digital actuales. Por ejemplo, la computación en la nube se ha convertido en un factor clave para el desarrollo de la inteligencia artificial (IA), ya que permite el despliegue de la IA a gran escala y proporciona la infraestructura necesaria para la mejora continua de los modelos de IA.

Cuadro 1. Computación en la nube frente a computación tradicional: resumen de las principales diferencias

	Tradicional	**Nube**
Propiedad y control	Propiedad y control directos de toda la infraestructura informática	Propiedad y gestión externas, acceso remoto
Escalabilidad	Menos flexible y automatizada, depende del *hardware* y la introducción manual	Elasticidad total, ajusta los recursos en función de la demanda

[1] Peter M. Mell y Timothy Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology (NIST), 28 de septiembre de 2011, https://doi.org/10.6028/NIST.SP.800-145.
[2] Nishant Kumar, “Cloud Computing vs Traditional Infrastructure: A Comparison", Marvsoft, 1 de enero de 2024, https://marvsoft.co/blog/view/cloud-computing-vs-traditional-it-infrastructure-a-comparison.

Modelo de costos	Gastos de capital	Gastos operativos
Mantenimiento, seguridad y actualización	Depende del personal informático dedicado *in situ*	Subcontratación a CSP

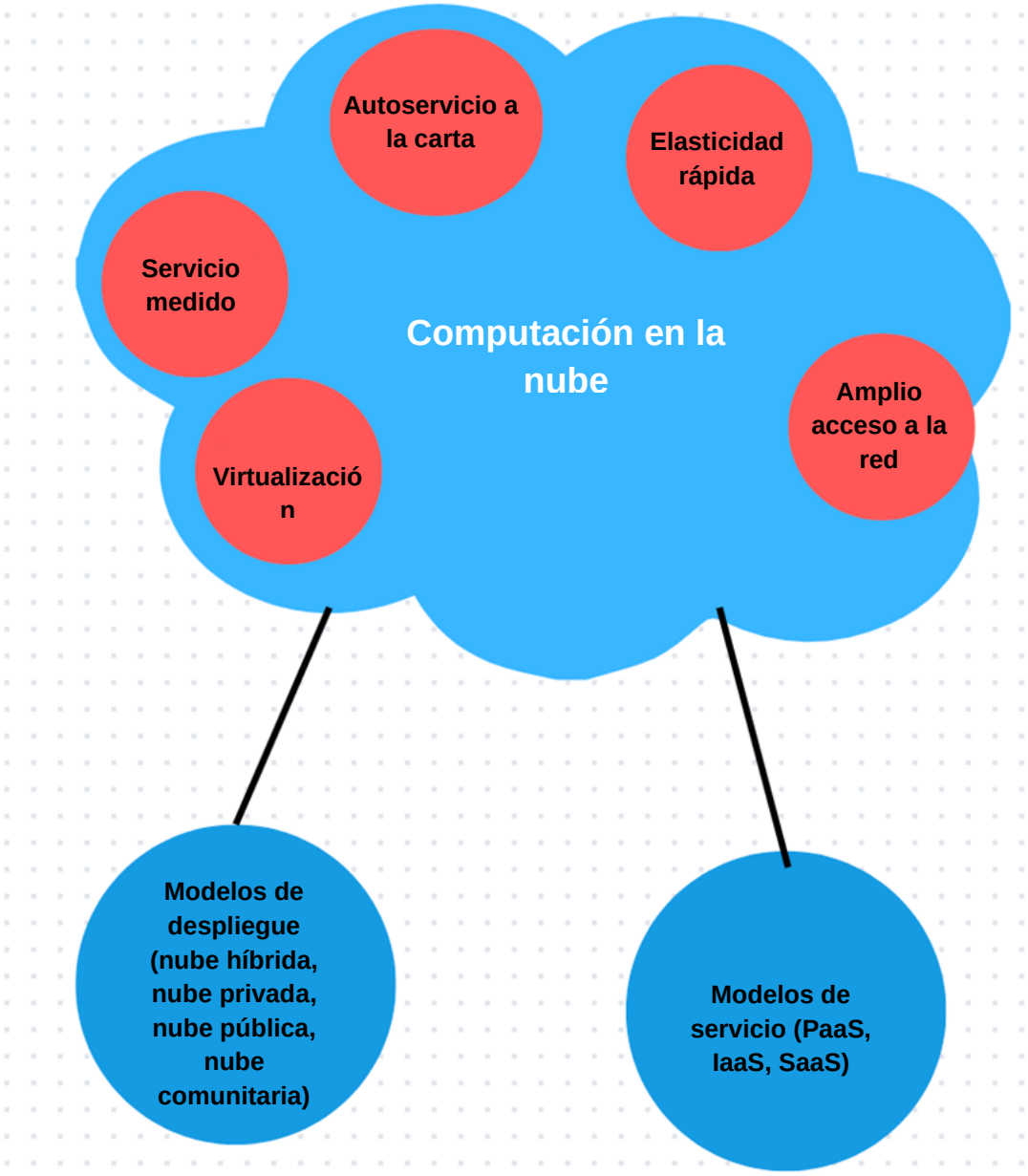

Figura 1. Componentes clave y modelos de despliegue y servicio de la computación en la nube

Hoy en día, la computación en la nube desempeña un papel fundamental en muchos sectores que se cruzan con la seguridad internacional. Estos abarcan desde las operaciones militares y de defensa hasta las infraestructuras críticas nacionales, así como las operaciones humanitarias.

Aunque la computación en la nube ofrece valiosas oportunidades y ventajas —entre ellas, la posibilidad de mejorar la seguridad internacional gracias a una mejor gestión de los datos y una mayor colaboración y eficacia operativa—, también conlleva algunos retos y riesgos. La figura 2 ofrece una visión general de algunos de los riesgos y oportunidades de la computación en la nube en el contexto de la seguridad internacional.

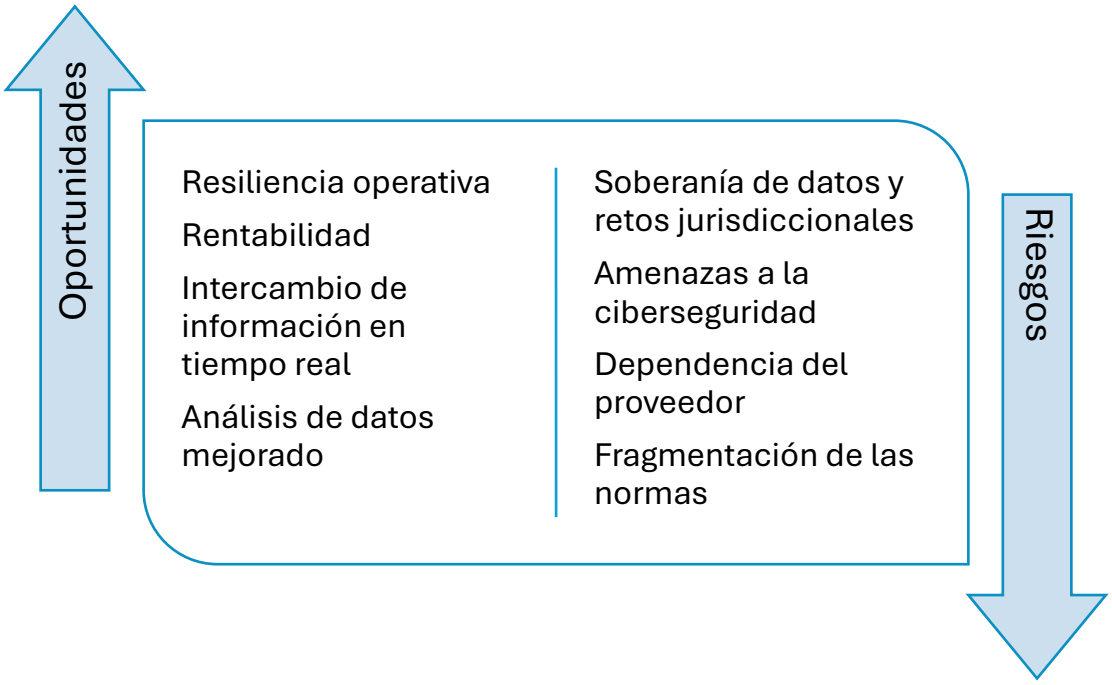

Figura 2. Oportunidades y riesgos de la computación en la nube para la seguridad internacional

Consulte el informe completo para obtener una descripción exhaustiva de las oportunidades y riesgos de la computación en la nube y sus implicaciones, así como una lista de las aplicaciones de computación en la nube pertinentes para la seguridad internacional.

2. Los retos de la gobernanza en el contexto de la seguridad internacional

La computación en la nube se ha convertido en una tecnología facilitadora esencial y en una importante capa subyacente de la economía digital mundial, con implicaciones para la paz y la seguridad internacional. De ello se deduce que su buena gobernanza es clave para maximizar los beneficios de la tecnología y minimizar sus riesgos. Sin embargo, aún no ha surgido un debate global y coherente sobre la gobernanza de la computación en la nube. Debido a algunos retos importantes, el panorama de la gobernanza de la computación en la nube ha sido, en cambio, fragmentado, incoherente y muy complejo. Estos retos se derivan de la naturaleza de la propia tecnología y del modelo de negocios que subyace a la computación en la nube, así como de factores vinculados a las realidades geopolíticas y de seguridad internacional con las que se cruza la computación en la nube.

La complejidad de la computación en la nube implica que es un sistema de tecnologías especialmente difícil de regular. Esto ha dado lugar a un complejo panorama regulatorio de políticas, legislaciones, buenas prácticas y normas que se empalman entre sectores, industrias y países. Aunque el alcance de la computación en la nube es mundial, **presenta niveles extremadamente altos de concentración geográfica y de mercado**. Esto tiene un efecto importante sobre la gobernanza, ya que confiere a unos pocos agentes del sector una gran influencia en los debates regulatorios, tecnológicos y de gobernanza.

Además, como las tecnologías no existen en silos, **la computación en la nube se cruza con los debates sobre gobernanza de otras tecnologías** (por ejemplo, cables submarinos, microchips e IA). Esto no solo significa que es difícil diseñar un esfuerzo cohesionado y centrado en torno a la computación en la nube, sino también que esta es a la vez un conjunto de tecnologías que hay que gobernar y una tecnología cuya gobernanza puede ponerse al servicio de la gobernanza —y de los objetivos de políticas— de otro conjunto de tecnologías. Esto es especialmente cierto en el contexto de la gobernanza de la IA. Además, la computación en la nube está profundamente entrelazada con los deseos de los Estados de reducir su dependencia de la tecnología extranjera y de limitar el flujo de datos fuera de sus territorios. Esto ha situado las consideraciones sobre la **soberanía digital** en el centro de los debates sobre la gobernanza de la computación en la nube y ha tenido un impacto sustancial en la configuración del panorama de la computación en la nube. Por último, existen retos legales y de gobernanza relacionados con el **creciente uso que hacen las fuerzas armadas de la computación en la nube para obtener capacidades de combate** y con la **prestación de servicios por parte de los CSP en escenarios de conflicto**.

La gobernanza de la computación en la nube saca a la luz las tensiones inherentes a un entorno digital mundial cada vez más interconectado y a unos requisitos de seguridad nacional aparentemente contrapuestos. Esto se ve exacerbado por la creciente importancia de las tecnologías digitales y la conectividad, así como de la competencia tecnológica mundial que se deriva de ello. Sería aconsejable un enfoque global más cohesionado de la gobernanza de la computación en la nube y la coordinación de enfoques, marcos y herramientas de gobernanza. Una mayor fragmentación del panorama de la gobernanza podría afectar negativamente a la seguridad, la protección y la resiliencia de la nube, y reducir la capacidad de la comunidad internacional para aprovechar los beneficios de la computación en la nube al tiempo que aborda sus riesgos.

El cuadro 2 ofrece una breve descripción de cada uno de estos retos y expone sus implicaciones. En el informe completo figura un análisis exhaustivo y más profundo de cada reto y sus implicaciones.

Cuadro 2. Retos de la gobernanza de la computación en la nube y sus implicaciones

Reto de gobernanza	**Descripción del reto**	**Implicaciones para la gobernanza de la computación en la nube**

Complejidad	La “nube” comprende una intrincada red de tecnologías (tanto de *hardware* como de *software*), servicios y agentes que operan a escala mundial en todos los sectores. Como tal, es un complejo sistema de sistemas de tecnologías con altos niveles de opacidad, en el que comprender las relaciones entre sus diversos elementos e identificar con claridad los nodos de riesgo resulta particularmente complicado.	• Complejidad, incoherencia, dificultad y fragmentación de las regulaciones y la gobernanza. • Panorama complejo para las empresas y los legisladores de hacer cumplir las regulaciones y la gobernanza de la nube. • Gran número de actores y mandatos entre distintos sectores, tecnologías y jurisdicciones. • Gran carga de cumplimiento para los CSP. • Posibles repercusiones negativas en la seguridad y la resiliencia de la nube.
Concentración geográfica y de mercado	A pesar de su naturaleza global, interconectada y compleja, la computación en la nube presenta niveles extremadamente altos de concentración de mercado. Los 10 mayores CSP se concentran en tres países, y los 3 primeros acaparan 65 % del mercado mundial.	• Concentración de la influencia sobre la tecnología y su gobernanza en solo unas cuantas empresas privadas. • Brecha de conocimientos entre el sector privado y los legisladores. • Opacidad en el funcionamiento y las prácticas de seguridad de los CSP. • Contribuye a la centralidad de la soberanía digital en los debates sobre gobernanza.
Intersección con otros esfuerzos de gobernanza tecnológica	La computación en la nube se cruza con una multitud de debates e iniciativas internacionales en materia de gobernanza, como los relativos a los cables submarinos, la IA, los microchips, las comunicaciones 5G y 6G, inclusive la gobernanza más amplia de internet y el ciberespacio. Cabe destacar la profunda integración de la computación en la nube en el debate más amplio sobre la gobernanza de la IA. De hecho, un debate emergente en la gobernanza de la IA sitúa la computación en la nube como un recurso en la caja de herramientas de la gobernanza de la IA. Estas propuestas	• Empalme con otros debates e iniciativas en materia de gobernanza. • Influencia de distintos debates, iniciativas y medidas de gobernanza adyacentes en el sector de la computación en la nube. • Creciente necesidad de intercambio entre las iniciativas de gobernanza en todos los campos tecnológicos.

	pretenden regular determinados aspectos de la IA —principalmente el acceso a la potencia informática y los microchips— a través de la "nube".	
Soberanía digital	La soberanía digital está en el centro de los debates sobre la gobernanza de la computación en la nube. Esto se debe principalmente a la concentración geográfica de los principales CSP en unos cuantos Estados, la naturaleza transfronteriza de la computación en la nube, el riesgo percibido de influencia extranjera y la importancia económica y de seguridad nacional de los datos en el siglo XXI. Por estas razones, la computación en la nube está en la mira de los Estados, con el fin de minimizar su dependencia de la tecnología extranjera y limitar el flujo de datos desde sus territorios.	• Mayor fragmentación normativa. • Entrelazamiento con la competencia geopolítica. • Diferentes normas de privacidad y seguridad de datos en los distintos Estados y regiones. • Mayor carga de cumplimiento para los CSP. • Posibles repercusiones negativas en otros objetivos de gobernanza. • Importante factor que moldea al sector de la computación en la nube.
Mayor uso en el ámbito militar	El creciente uso de soluciones de computación en la nube en el sector militar y, en un sentido más amplio, por parte de todos los actores implicados en la seguridad nacional, no solo tiene implicaciones para la seguridad internacional, sino que también plantea retos para la gobernanza. El creciente uso de la computación en la nube para proporcionar capacidades de combate por parte de las fuerzas armadas tiene implicaciones directas. También hay problemas de gobernanza relacionados con la prestación de servicios digitales por parte de los CSP en tiempos de conflicto.	• Línea difusa entre tecnología militar y civil. • Creciente centralidad, dependencia e influencia de las empresas tecnológicas en los conflictos y asuntos militares. • Implicaciones para el derecho internacional humanitario y consecuencias en cascada sobre personas e infraestructuras civiles. • Fomenta el deseo de soberanía digital, aumentando la dificultad de la cooperación.

3. Implicaciones para el control de armamento

Las implicaciones de la computación en la nube se extienden al ámbito del control de armamento por dos razones principales. En primer lugar, la computación en la nube es cada vez más un método

clave a través del cual se almacenan y comparten capacidades digitales, intangibles y de doble uso, así como el acceso a ellas. Estas capacidades también se desarrollan mediante el acceso remoto a una gran cantidad de potencia informática. En segundo lugar, gran parte de la infraestructura digital mundial depende del funcionamiento y la integridad de los servicios de computación en la nube.

Esto implica dos objetivos clave para el control de armas en el contexto de la computación en la nube:

1. **Proteger la "nube":** la computación en la nube y la infraestructura relacionada forman una capa crítica de la sociedad y la economía y son un elemento facilitador de la conectividad y la innovación digital. Por lo tanto, debe protegerse.
2. **Desarrollo de "gemelos digitales" de conceptos de control de armamento para la "nube":** [3] la computación en la nube puede utilizarse para acceder y desarrollar capacidades digitales o para trasladar y acceder a información digital sujeta a disposiciones de control de armamento. Así pues, los mecanismos de control de armamento deberían dar a la comunidad internacional la capacidad de supervisar con efectividad este uso que se hace de la nube.

El Cuadro 3 describe estos objetivos y las formas de avanzar.

Cuadro 3. Implicaciones de la computación en la nube para el control de armamento

Proteger la nube	**Desarrollar "gemelos digitales" de los mecanismos de control de armamento**
La cuestión: La computación en la nube está cada vez más integrada en todos los estratos de la economía mundial y se está haciendo vital para el funcionamiento de sectores críticos. Las fallas, ya sean accidentales o como resultado de una acción adversa, tendrían consecuencias graves para toda la sociedad.	**La cuestión:** Las realidades tecnológicas de la computación en la nube ponen a prueba la lógica de los conceptos tradicionales de control de armas y su capacidad para ser efectivos. Estos conceptos (por ejemplo, el control de las exportaciones) se centran en la territorialidad y el control de los objetos físicos y sus movimientos. Como tales, tienen dificultades para abordar el flujo dinámico y sin fronteras de los datos gracias a la computación en la nube o para hacer frente al riesgo de proliferación de capacidades disruptivas de IA habilitadas por el acceso remoto a una gran cantidad de potencia informática.

[3] En el contexto de esta reseña, "gemelo digital" no se refiere a una réplica virtual de un objeto físico, sino a un equivalente de las herramientas y mecanismos de control de armas, pero mejor adaptado a las características del mundo digital.

El camino por seguir: El control de armamento no se limita a la gestión de sistemas de armas, sino que también se ocupa de comportamientos y normas. Por lo tanto, debe surgir una conversación global que esboce un conjunto común de expectativas, normas y comportamientos entre los Estados con respecto a la computación en la nube y la infraestructura relacionada. En el ámbito cibernético, esto comienza con la aplicación de compromisos en el marco de un comportamiento estatal responsable en el uso de las tecnologías de la información y la comunicación (TIC). Dado que la computación en la nube no es solo una cuestión de ciberseguridad, debería establecerse un conjunto similar de expectativas, comportamientos y normas en torno a los ataques físicos a los servicios e infraestructuras en la nube. También debería haber acuerdos comunes similares con respecto al uso que hacen las fuerzas armadas de los servicios de computación en la nube.	**El camino por seguir:** La capacidad de la comunidad internacional para hacer frente a los retos de la creciente prevalencia de la computación en la nube que plantea para el control de armamento dependerá en gran medida de su capacidad para desarrollar "gemelos digitales" de diversos conceptos y mecanismos de control de armamento para el mundo digital. En el caso de los controles de las exportaciones, por ejemplo, se requiere el desarrollo de nuevas formas de hacer operativo el "control" en el contexto desmaterializado de la computación en la nube. Para ello es necesario comprender qué conceptos y herramientas pueden tener mayor impacto a la hora de gestionar el acceso remoto a gran cantidad de potencia informática. Las futuras investigaciones deberían explorar cómo pueden aplicarse otros conceptos (por ejemplo, los requisitos de licencia) a este fin. También va a ser necesaria una mayor armonización internacional en este ámbito.

4. Conclusiones

La comunidad internacional debería tratar de reducir la fragmentación del panorama de la gobernanza de la computación en la nube con el fin de alinear y harmonizar mejor los planteamientos de la gobernanza. Un marco único de gobernanza para la computación en la nube podría no ser alcanzable o deseable. Sin embargo, una mayor coordinación e interoperabilidad internacional entre los marcos de gobernanza ayudará a minimizar las lagunas y contradicciones entre estos. Esto ayudará a fomentar un planteamiento global más cohesionado y propicio para garantizar la seguridad, la protección y la resiliencia de la “nube”.

Es necesaria una comprensión y una exploración más profunda del impacto de la computación en la nube en el control de armamento para evitar que sus características únicas se utilicen para que sigan proliferando tecnologías disruptivas de doble uso. Es necesario un debate multilateral centrado en la protección de la nube, así como el desarrollo de "gemelos digitales" de diversas herramientas de control de armamento para las realidades de la computación en la nube. Esto debería complementarse con nuevas investigaciones sobre qué herramientas existentes y nuevas (por ejemplo, requisitos de licencia) pueden utilizarse en el contexto del control de armamento para la computación en la nube. En el futuro, este esfuerzo no debería limitarse a la computación

en la nube, ya que las nuevas tecnologías van a seguir poniendo a prueba la efectividad de las herramientas tradicionales de control de armamento.

Los Estados deberían profundizar en el debate sobre la computación en la nube en el contexto de las discusiones multilaterales sobre la seguridad internacional de las TIC. Este debería incluir un análisis de los retos específicos y de en qué medida el marco existente es capaz de abordarlos. También debe incluir un análisis de las oportunidades únicas que ofrece la computación en la nube para ayudar a los Estados en la aplicación de los compromisos existentes e impulsar la ciber resiliencia nacional.

Es necesario un verdadero enfoque multilateral para debatir, diseñar y aplicar respuestas políticas adecuadas a los retos de la computación en la nube. Un elemento importante, y muy recomendable, de este enfoque debería ser la participación significativa de un grupo geográficamente representativo de los actores de la industria activos en este ámbito en tales debates. Lo mismo cabe decir de los representantes del mundo académico, la sociedad civil y la comunidad técnica, incluidos los investigadores de temas de seguridad y los encargados de responder a incidentes.