Ciberespacio, soberanía y derecho internacional

Oscar Niss [0009-0004-3806-8278]

[1] Maestrando en Derecho Internacional, Universidad Empresarial Siglo 21, Córdoba, Argentina
[2] Ministerio de Gobierno, Provincia de Buenos Aires, Argentina

oscarniss@gmail.com

Resumen. El presente trabajo analiza la aplicabilidad del Derecho Internacional Público en el ciberespacio, con foco en la noción de soberanía digital y la creciente utilización del entorno cibernético como escenario de conflicto interestatal. A través de casos paradigmáticos —como los ciberataques a Estonia (2007), la operación Stuxnet (2010), la interferencia electoral en Estados Unidos (2016) y las operaciones híbridas en Ucrania (2014–2017)— se exploran las limitaciones de los marcos normativos actuales frente a la atribución, regulación y respuesta a ciberoperaciones. El artículo examina, además, la evolución del ciberespacio como dominio operacional para las Fuerzas Armadas y los esfuerzos normativos realizados desde organismos como la ONU, la OTAN y actores estatales. Se concluye que la ausencia de mecanismos jurídicos vinculantes, sumada a la necesidad de infraestructura tecnológica soberana, requiere repensar la relación entre capacidad técnica y normativa en un entorno globalizado y transnacional. El despliegue de tecnologías nacionales como los IXP, BGP y AS podría fortalecer la soberanía digital y facilitar la aplicación del derecho internacional.

Palabras clave: Ciberespacio, Soberanía, Derecho Internacional, Ciberoperaciones, Conflictos Híbridos

Cyberspace, sovereignty, and international law

Abstract. This paper analyzes the applicability of Public International Law in cyberspace, focusing on the concept of digital sovereignty and the increasing use of the cyber domain as a theater for interstate conflict. Through emblematic case studies—such as the cyberattacks on Estonia (2007), the Stuxnet operation (2010), electoral interference in the United States (2016), and hybrid warfare in Ukraine (2014–2017)—it explores the limitations of current legal frameworks regarding attribution, regulation, and response to cyber operations. The article further examines the evolution of cyberspace as an operational domain for armed forces and the normative efforts by organizations such as the UN, NATO, and individual states. It concludes that the lack of binding legal mechanisms, along with the necessity for sovereign technological infrastructure, demands a reconsideration of the relationship between technical capacity and international norms. The deployment of national technologies such as IXP, BGP, and AS systems

could strengthen digital sovereignty and support the enforcement of international law.

Keywords: Cyberspace, Sovereignty, International Law, Cyberoperations, Hybrid Conflicts

1 Introducción

El Ciberespacio ha emergido como un campo crítico para las relaciones internacionales, desafiando las nociones tradicionales de soberanía y control estatal. Al mismo tiempo, la infraestructura técnica que soporta el Ciberespacio — fundamentalmente física y geográficamente localizada — resalta las tensiones entre la virtualidad de Internet y la territorialidad de las naciones.

El Derecho Internacional Público (DIP) ha tratado de adaptarse a estos desafíos con iniciativas como el Manual de Tallin, que ha sido clave en la orientación sobre ciberseguridad y ciberdefensa, aunque es un tratado académico y no vinculante. Además, la ONU, a través de sus diversos mecanismos, sigue evaluando cómo aplicar las normas de soberanía del siglo XXI en un espacio digital globalizado.

La soberanía en el Ciberespacio plantea desafíos singulares debido a las dificultades inherentes a la atribución de ciberataques, las discrepancias en la interpretación de la Carta de las Naciones Unidas y la creciente interdependencia tecnológica, que ha llevado a países como Rusia a proponer marcos legales exclusivos para el ciberespacio, mientras otros como el Reino Unido apelan a las normas actuales que lo regulan.

Cabría entonces preguntarnos ¿Alcanzan los actuales instrumentos del derecho internacional público para normar la soberanía en el Ciberespacio? ¿Están considerando estos debates las nuevas tecnologías y los intereses en juego? ¿Se requiere del despliegue de tecnología de cada Estado, que demarque señalar los límites o confines de espacio cibernético soberano, como se hizo con cada dominio tradicional?

2 Casos de estudio

En los casos que presentaremos a continuación se evidencia el problema de la soberanía en el ciberespacio, reflejado en la limitada capacidad de los Estados para ejercer control —tanto técnico como normativo— sobre su territorio digitalizado. A pesar de los avances impulsados desde 2010 por los Grupos de Expertos Gubernamentales (GGE)[1] y, más recientemente, por los Grupos de Trabajo de Composición Abierta (OEWG)[2] en el marco de las Naciones Unidas, así como del desarrollo de tratados académicos como el

[1] United Nations. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. Disponible en: https://undocs.org/A/70/174

[2] United Nations. (2021). *Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (2019–2021)*. A/75/816. Disponible en: https://undocs.org/A/75/816

Manual de Tallin[3], persiste la falta de consenso respecto a la aplicación del derecho internacional en este nuevo dominio. Esta situación deja una brecha significativa en la protección jurídica de los Estados frente a las amenazas y agresiones cibernéticas.

2.1 Estonia (2007)

El Ciberataque a Estonia en 2007 marcó un hito en la historia de los conflictos cibernéticos. Este ataque, atribuido a actores rusos, afectó gravemente las infraestructuras críticas de Estonia, incluidas sus redes bancarias, gubernamentales y de comunicaciones. El incidente reveló la vulnerabilidad de un Estado a Ciberataques masivos, planteando serios problemas para la soberanía. Estonia, al no contar con un marco legal robusto para gestionar este tipo de amenazas, tuvo que buscar ayuda en organizaciones internacionales como la OTAN.

Posteriormente, en Estonia se estableció el Centro de Excelencia en Ciberdefensa que promovió la creación de normas internacionales para la protección cibernética. Aunque no hubo una resolución formal en tribunales internacionales, este caso subrayó la importancia de la soberanía en el ciberespacio, al destacar que las naciones deben tener control sobre sus infraestructuras tecnológicas.

2.2 Stuxnet (2010)

En el caso de Stuxnet (2010), un sofisticado malware informático dirigido a las instalaciones nucleares de Irán mostró cómo un ataque cibernético patrocinado por un Estado puede socavar la soberanía de otro país. A diferencia del ataque en Estonia, Stuxnet habría sido diseñado por los EE.UU. – también se señala a Israel - específicamente para dañar una instalación estratégica en particular, lo que generó un debate sobre los límites de la soberanía cibernética y el uso de Ciberarmas en el contexto de conflictos armados.

Aunque no hubo una respuesta internacional formal, este incidente resaltó la necesidad de un marco normativo global para regular el uso de Ciberoperaciones ofensivas.

2.3 EEUU (2016)

La presunta interferencia en las elecciones presidenciales de Estados Unidos en 2016 constituyó un desafío relevante a la soberanía estatal, en particular al derecho soberano de los pueblos a elegir libremente a sus gobernantes. De acuerdo con diversas agencias de inteligencia, actores vinculados al Estado ruso habrían desplegado campañas de

[3] El Manual de Tallin sobre el derecho internacional aplicable a la guerra cibernética es un estudio académico no vinculante sobre cómo se aplica el derecho internacional en este tipo de conflictos, fue patrocinado por el Centro de Excelencia en Defensa Cibernética Cooperativa (CCDCOE, por sus siglas en inglés) De la OTAN en 2009, el documento estuvo a cargo de 20 expertos en derecho internacional.

desinformación y operaciones de intrusión informática con el objetivo de influir en el proceso electoral y socavar la confianza en las instituciones democráticas[4].

Aunque no se logró demostrar fehacientemente que estas acciones alteraran el resultado final ni atribuir de forma concluyente su autoría al gobierno ruso, la injerencia en el proceso electoral de un Estado soberano provocó una profunda crisis diplomática y fue considerada una violación a los principios establecidos en la Carta de las Naciones Unidas. A pesar del intento de imponer de sanciones y otras medidas por parte del gobierno estadounidense, la ausencia de un mecanismo internacional específico para abordar este tipo de agresiones dejó la controversia sin una resolución jurídica definitiva.

2.4 Ucrania – Rusia (2014)

El conflicto entre Ucrania y Rusia, particularmente a partir de 2014 con la anexión de Crimea, constituye un ejemplo paradigmático de cómo el ciberespacio se ha integrado como un campo de operaciones en disputas geopolíticas. Diversos ataques cibernéticos dirigidos a infraestructuras críticas ucranianas, atribuidos a actores vinculados al Estado ruso, revelan el uso estratégico de herramientas digitales para desestabilizar un Estado soberano. Uno de los episodios más relevantes fue el despliegue del malware NotPetya en 2017[5], que afectó gravemente sistemas gubernamentales, financieros y de transporte, y cuyas consecuencias se extendieron incluso a nivel global.

Estos ciberataques, que posteriormente avanzaron con operaciones militares convencionales, reflejan el carácter híbrido de los conflictos contemporáneos, donde se combinan acciones cinéticas con operaciones cibernéticas de amplio alcance.

3 El Ciberespacio como ambiente operacional de las Fuerzas Armadas

El Ciberespacio ha evolucionado rápidamente desde su creación, convirtiéndose en un nuevo dominio operativo para los Estados, en particular para las Fuerzas Armadas, con capacidades que permiten a los Estados desarrollar operaciones cibernéticas, tanto defensivas como ofensivas. El concepto de ambiente operacional está configurado por varios marcos teóricos y prácticos, destacando el Manual de Tallin y otros documentos normativos y académicos clave.

[4] Office of the Director of National Intelligence (ODNI). (2017). *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*. ICA 2017-01D. Disponible en: https://www.dni.gov/files/documents/ICA_2017_01.pdf

[5] Greenberg, A. (2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Wired. Disponible en: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

3.1 La topología del Ciberespacio

El Ciberespacio es entendido en términos generales como un dominio global de infraestructura de información, compuesto por redes, servidores, dispositivos y sistemas interconectados. Esta definición es clave cuando se considera la seguridad y operatividad de las Fuerzas Armadas, pues, si bien el Ciberespacio es un entorno físico y virtual, tiene implicaciones muy reales en la defensa y proyección de la soberanía de un Estado.

El Manual de Tallin, establece desde sus primeros párrafos que el Ciberespacio debe ser considerado un dominio de guerra en la misma categoría que el aire, el mar y la tierra. Esto significa que las Fuerzas Armadas deben poder operar en el Ciberespacio de manera similar a cómo lo hacen en otros dominios operacionales, con capacidades de defensa y ataque, aunque con desafíos propios debido al componente de naturaleza virtual y transnacional del Ciberespacio.

3.2 Las reglas de la Ciberguerra

El Manual de Tallin (2013 / 2017) en su Regla 1 afirma que los principios del Derecho Internacional aplicables a los conflictos armados son igualmente válidos en el Ciberespacio, lo que implica que los ataques cibernéticos, así como las defensas cibernéticas, deben cumplir con las normas internacionales de proporcionalidad, distinción, y necesidad. En este sentido, el Ciberespacio no es solo un medio para la comunicación o intercambio de información, sino también un teatro de operaciones militares.

Además, se destaca la importancia de infraestructuras críticas dentro del Ciberespacio, como los sistemas de mando y control de las Fuerzas Armadas, que son esenciales para la conducción de operaciones militares. El ataque o la alteración de estas infraestructuras puede tener consecuencias devastadoras, afectando la capacidad de respuesta de un Estado en un conflicto. Por lo tanto, las Fuerzas Armadas deben asegurar sus propios sistemas cibernéticos y contar con estrategias de ciberdefensa bien establecidas.

4 Debates sobre el Derecho Internacional Público en el Ciberespacio

Diversos trabajos en ámbitos como la Organización de las Naciones Unidas, la Organización de Estados Americanos, la Organización del Tratado del Atlántico Norte y diversas naciones, han debatido los aspectos soberanos del Ciberespacio.

El manual de Tallin aborda, además, cómo el derecho el Derecho Internacional Humanitario (DIH) y el Derecho Internacional Consuetudinario, se aplica a los conflictos y operaciones en el Ciberespacio. Este texto considera que el Ciberespacio no es un "territorio sin ley", afirmando que las normas del derecho internacional, incluyendo la Carta de las Naciones Unidas, son aplicables y que los Estados tienen soberanía sobre su infraestructura de información y comunicación dentro de su territorio. En ese sentido, las Ciberoperaciones pueden constituir una violación de la soberanía si se llevan a cabo sin el consentimiento del Estado afectado.

Por otro lado, han existido tres Grupos de Expertos Gubernamentales y sucesivos Grupos de Trabajo de Composición Abierta, que han examinado las amenazas existentes y potenciales en el ámbito Cibernético, publicando en 2010, un primer informe donde consideran que los Estados deben observar, entre otros principios de derechos internacionales, la soberanía del Estado, la solución de controversias por medios pacíficos, y el tema de no intervenir en los asuntos internos de otros Estados.

Además, las naciones se han expresado en similar sentido, como la Argentina, mediante Resolución del Ministerio de Defensa 105/2023, diciendo que hay "un subconjunto de la infraestructura del Ciberespacio que podemos conceptualizarla como cuota que atraviesa al sistema de defensa nacional ya que es utilizado por las organizaciones que lo conforman para el cumplimiento de sus misiones y funciones" (Ministerio de Defensa Argentina,2022). La misma resolución continúa diciendo que es necesario el resguardo soberano del mismo, asegurando las operacionales de los sistemas de mando y control, incluido los sistemas de armas que por su tecnología así lo requieran.

Diversos autores también han trabajado el tema, extendiendo el concepto considerando que "las nuevas formas de regulación vinculadas al diseño y producción de tecnologías digitales también afectan los principios de autonomía, soberanía y defensa de los intereses nacionales y regionales." (Vercelli, 2016). Este concepto extendido de la soberanía más allá de lo territorial suma más complejidad al tema obligando a pensar en infraestructuras de comunicaciones y almacenamiento que permitan ese ejercicio pleno de soberanía.

5 Conclusiones: Las adecuaciones tecnológicas y normativas van de la mano

Normar cuestiones tecnológicas, conllevan un trabajo interdisciplinario dinámico y en permanente adecuación, sobre todo en tiempos donde los ciclos de innovación, producción y puesta en el mercado de tecnología son altamente dinámicos. Los informes, tanto de los GGE y los OEWG, estarían omitiendo el análisis de cuestiones tecnológicas que podrían determinar límites a las normas del derecho internacional.

En ese sentido algunas naciones han trabajado estas cuestiones avanzando en despliegues de infraestructura TIC que podrían facilitar los aspectos normativos. El uso de infraestructuras que administran Protocolos de Borde de Internet (BGP por sus siglas en ingles), el enrutamiento entre sistemas autónomos (AS) y las estrategias para proteger los servicios esenciales del estado detrás de sus IXP (Puntos de Intercambio de Internet), podrían facilitar la aplicación de normativas legales domésticas, contribuyentes al derecho internacional. Países como Estonia, Corea del Sur, Alemania, Rusia, Brasil entre otros, fomentan normas legales disponiendo que el tráfico de servicios esenciales - como salud, defensa, energía y finanzas - se mantenga dentro de sus fronteras, utilizando IXP nacionales – intramuros-, cuestión que reduce la dependencia de servidores extranjeros y minimiza el riesgo de interrupciones o ataques.

Disponer, técnica y normativamente, servicios esenciales o de interés del Estado, en infraestructura de este tipo, permitiría, no sólo una mejora sustancial al ejercicio de la

soberanía digital, sino un resguardo legal ante intrusiones de otros Estados en su dimensión de Ciberespacio soberano.

Referencias

ARG DCTO-2021-457-APN-PTE. (s.f.). Directiva de Política de Defensa Nacional2021.
Buchan, R. The Rights to Privacy and Data Protection in Times of Armed Conflict (2022). NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).
C., B. (2013). Aproximación a la noción de soberanía estatal en el marco del proceso andino deintegración. Revista Republicana.
Carrillo, M. R. (2023). LA ARTICULACIÓN DE LA SOBERANÍA DIGITAL EN EL MARCO DE LA UE. Revista de Derecho Comunitario Europeo, 75, mayo-septiembre, 133-171.
CCN-CERT. (2023). Recomendaciones de Protección del Dato en la Nube: Soberanía Digital.
ITU. (2016). Tecnologías digitales para el cumplimiento de los Objetivos de Desarrollo Sostenible de las Naciones Unidas. Obtenido de https//:itu.int
Lopez, J. Setola, R. Wolthusen S. Critical Infrastructure Protection (2012).
Madiega, T. (2020). Digital Sovereignty for Europe: Enhancing Strategic Autonomy in the Digital Field.
Ministerio de Defensa Argentina Resol-105-2023. (2022). Política de Ciberdefensa Argentina. Argentina.
Niss, Oscar. Ciberdefensa para Armar: Derecho Internacional, Soberanía, Diplomacia y Estrategia Militar (2025) ISBN-13: 979-8291102305 https://www.amazon.com/dp/B0FGX3BD61
ONU A/65/201. (2010). Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones.
ONU A/70/174. (2015). Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.
ONU-A/77/287. (2022). Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales.
Society, I. (2022). Explorando la Soberanía Digital.
Tallinn Manual. (2013). The NATO Cooperative Cyber Defence Centre of Excellence. Tallin: CAMBRIDGE UNIVERSITY PRESS. The NATO Cooperative Cyber Defence Centre of Excellence. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.
Vercelli, A. “Repensando los bienes intelectuales comunes”, Universidad Nacional de Quilmes - Tesis de doctorado con mención en Ciencias Sociales y Humanas (2009).