Aportes Teóricos a la Geopolítica Regional del Ciberespacio

Leandro Ocón

Las amenazas en el ciberespacio presentan algunos de los mayores desafíos del siglo XXI. En múltiples ocasiones se ha demostrado que exponen la vulnerabilidad de los sistemas electorales, las infraestructuras críticas y hasta la economía global (Nye, 2010; 2016, Libicki, 2016; Singer y Brooking, 2019; Ocón, 2019, Gastaldi y Ocón, 2021). Es por ello que, más allá de los esfuerzos que se puedan realizar a nivel individual, el ciberespacio demanda una política integral de ciberdefensa que tenga alcance nacional y regional.

La amplitud del internet se ha incrementado aún más durante la pandemia COVID-19. Las respuestas gubernamentales a la crisis de salud fueron, principalmente, ancladas a políticas orientadas al confinamiento. Dicha circunstancia benefició notablemente a la industria digital, particularmente a las llamadas *Big Tech* o las "Gigantes Tech" norteamericanas (Facebook, Apple, Microsoft, Amazon y Google) y a las de origen chino (Tencent y Alibaba). En América Latina, Mercado

Libre se posicionó como la empresa con mayores tasas de crecimiento, superando incluso a Petrobras y a Itaú.

En este sentido, los albores del siglo XXI se presentan con una aceleración de la expansión ciberespecial, las nuevas tecnologías de la comunicación, la convergencia digital, el internet de las cosas (IoT), acompañados por instrumentos tales como la inteligencia artificial, la matemática algorítmica, las redes sociales, la programación y la industria de semiconductores. Todo ello se lo identifica como parte de una nueva fase de la Revolución industrial, ya en su cuarta y/o quinta etapa. El ciberespacio se ha constituido en uno de los principales "espacios" de interacción entre seres humanos, de ocio y hasta de producción económica. Dentro de esta lógica, se presenta como un dominio donde hay intereses individuales, nacionales, regionales y globales en una compleja dinámica de competencia y cooperación, donde se observan situaciones de conflicto y de paz. Incluso, considerando los aportes de Farrell y Newman (2016), se puede afirmar que las características propias del dominio ciberespacial favorecieron a una "armamentización de la interdependencia". En términos de los autores, se puede pensar cómo la globalización económica crea su propio conjunto de estructuras internacionales —a través de redes globales— generando nuevas formas de poder estatal y no-estatal.

La "espacialidad" del Ciberespacio

Uno de los principales desafíos que se presentan a la hora de abordar el ciberespacio es comprender qué es y cómo funciona. Si bien existen múltiples definiciones de lo que es el ciberespacio, se propone utilizar la ofrecida en "Abracadabra y la Biblioteca de Babel: Una aproximación geopolítica a la espacialidad del ciberespacio" (Ocón, 2021):

> El ciberespacio es un espacio cognitivo anclado en una esfera física y una lógica, donde tiene lugar las representaciones y las dinámicas de estas espacialidades. En este sentido el ciberespacio es un universo constituido sobre la base del lenguaje en su aspecto técnico-físico y cognitivo. (p.40)

De la definición mencionada se pone de manifiesto la "transversalidad" del ciberespacio en múltiples dimensiones o capas. Es decir, el

ciberespacio no es meramente una dimensión de realidad virtual o de realidad "aumentada", es un espacio de relacionamiento cognitivo mediado por dispositivos técnicos y mecanismos cognitivos de vinculación basados en el lenguaje.

Dicha propuesta surge de los aportes de Libicki (2009) que consisten en una aproximación por capas integradas verticalmente, que permiten plantear un abordaje teórico y gráfico a la transversalidad del ciberespacio. En suma, las condiciones de existencia del ciberespacio se dan a partir de diversas capas o dimensiones que hacen posible su existencia.

En definitiva, lo aquí propuesto pretende visibilizar dos caras de una misma moneda. Por un lado, una física, es la que se encuentra compuesta por todos los dispositivos técnicos o hardware, tales como routers, cables, satélites y, la otra, una cara "semántica" que se entiende como la dimensión en la cual la información adquiere significado para los seres humanos. Tal como señala Sheldon (2015), lo "semántico" involucra un aspecto cognitivo. De esta manera, y siguiendo los argumentos de Libicki (2009) y Sheldon (2015), se puede afirmar que existen cuatro "capas" que hoy suponen dimensiones en las cuales el ser humano puede accionar influyendo en el ciberespacio: la capa o esfera físico-geográfica, la de la infraestructura física, la dimensión lógica-digital y finalmente el ciberespacio. El orden determina un punto central, las anteriores dan lugar a las posteriores. Es decir, el ciberespacio existe a partir de la dimensión lógico-digital y, al mismo tiempo, esta última se apoya en la existencia de infraestructura física, y así sucesivamente (ver Figura 1).

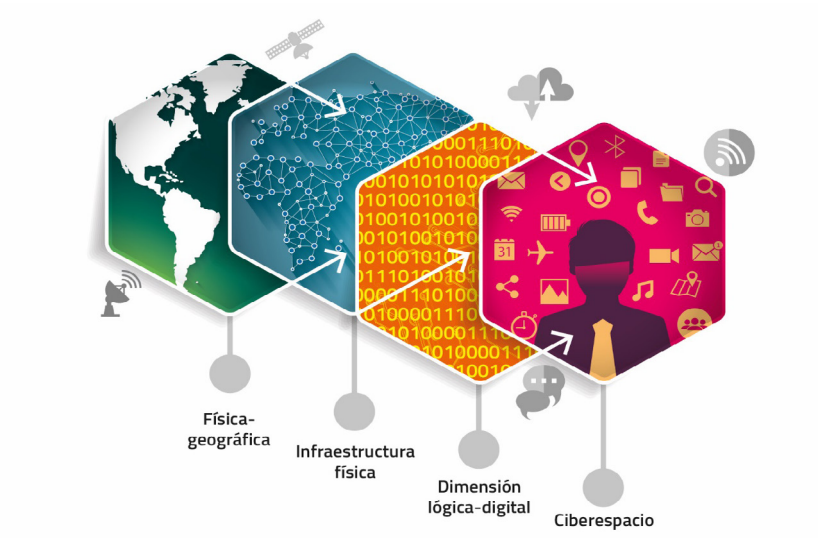


Figura 1: Las capas del Ciberespacio. Fuente: Ocón (2021)

Estado y Mercado del Ciberespacio

Muchas de las cuestiones anteriormente mencionadas son analizadas en "Ciberdefensa: Claves para una pensar una estrategia de Soberanía Nacional" (Gastaldi y Ocón, 2021). Observamos que existen una amplia variedad de políticas orientadas al ciberespacio que varían según condiciones estructurales previas de cada país y cuáles manifiestan sus objetivos estratégicos. Incluso, las definiciones de lo que es el ciberespacio varían según cada caso.

Ahora bien, como la dinámica ciberespecial se encuentra en constante transformación, en los próximos años, se definirán, entre las distintas naciones, regiones y/o bloques, nuevas políticas de ciberdefensa en torno a la privacidad, la libertad en internet, la regulación de los mercados digitales y la de infraestructuras críticas.

Considerando entonces, que el ciberespacio se encuentra en contaste cambio, también se identifican nuevas aproximaciones en constante evolución. La Unión Europea es un referente de instrumentación po-

lítica de alcance regional. Ejemplo de ello, es que el 16 de diciembre de 2020, la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una nueva Estrategia de Ciberseguridad. Dentro de la amplia gama de cuestiones que busca atender la Unión Europea en el ciberespacio, se encuentra la privacidad de sus ciudadanos, la libertad en el internet, la regulación de las empresas de tecnología de la comunicación y la cuestión de la infraestructura física.

En los últimos años se ha comenzando a poner el acento en la capa de la infraestructura física, particularmente los grandes centros de datos, la protección y ubicación de los cables submarinos y/o la tecnología 5G -y eventualmente 6G.

Por su parte, la nueva administración norteamericana presidida por Joe Biden, presentó diversos proyectos en torno a la regulación de los monopolios de las *Big Tech*. El mensaje fue claro al elegir en puestos claves a Lina Khan y Timothy Wu, ambos profesores de la Universidad de Columbia especializados en Derecho de la Competencia.

También, frente a los desafíos geopolíticos del ciberespacio, principalmente la injerencia en elecciones por parte de actores tales como China o Rusia, se estaría conformando una estrategia de gran alcance que involucraría organismos internacionales y regionales de distintas partes del globo (Fidler, 2021).

En las últimas décadas se ha complejizado la relación entre la ciudadanía, las redes sociales y la democracia, a tal punto que no pueden ser pensadas disociadas de una estrategia de Defensa Nacional (Ocón, 2019). Hay un amplio reconocimiento por parte de diversas figuras políticas y académicas que señalan el paulatino estancamiento en la carrera de poder ciberespacial por parte de Estados Unidos (Nye, 2017), no es de extrañar que desde el año 2015 Ted Koppel se pregunta "¿Dónde está el plan de ciberdefensa norteamericano?" Incluso las criptomonedas se presentan como un desafío a la hegemonía del dólar (Bloomberg, 2021). De esta forma, una política de Ciberdefensa de alcance global es uno de los principales desafíos de Joe Biden, en su intento de consolidar su proyecto de renovación democrática en el mundo. En este sentido, el análisis de escenario no es errado: no se

puede pensar, en el siglo XXI, la democracia y el desarrollo económico disociados del ciberespacio.

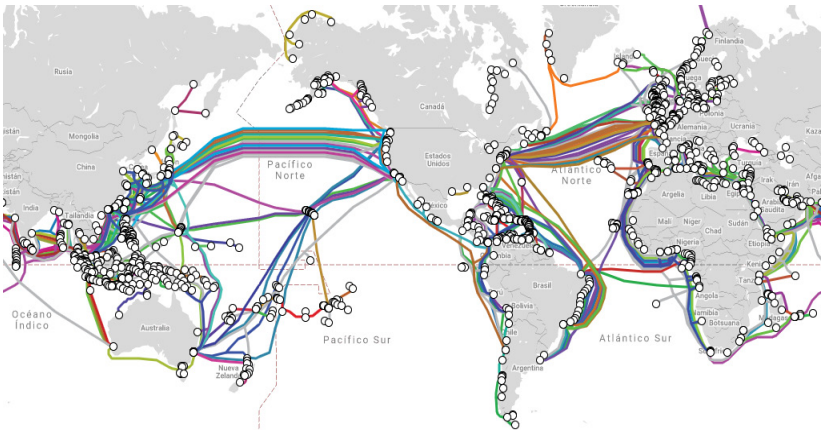
En el caso de América Latina dichos debates resultan prioritarios en el escenario pandémico y pospandémico. Así como el COVID-19 aceleró los procesos de digitalización de los países en la región, también es necesario apresurar los procesos de planificación y elaboración de estrategias, políticas e instrumentos relacionados a la ciberdefensa.

Aparte de los debates en torno a la privacidad, el uso de datos personales de usuarios y la expansión de los mercados de las *Big Tech* y las Fintech, es prioritario poner el foco en las infraestructuras críticas conectadas al ciberespacio y las que lo hacen posible: cables submarinos, servidores o centros de datos, tecnologías "G", entre otros. Esto no implica, necesariamente, poner freno a las empresas locales, todo lo contrario, el apoyo al crecimiento de las industrias y empresas nacionales y regionales puede favorecer a un mejoramiento de las capacidades políticas y económicas de la región.

Particularmente, cabe destacar, tal como señala Starosielski (2015), que los cables submarinos de fibra óptica son infraestructuras críticas que respaldan a nuestra sociedad de red global. Estos llevan el 99 % de todas las comunicaciones digitales transoceánicas (llamadas telefónicas, mensajes de texto, correo electrónico, sitios web, imágenes digitales y video). Es decir, son estos sistemas de cable, no los satélites, los que transportan la mayor parte de la información (de)codificada en todo el mundo. Desde el punto de vista estratégico, estos cables submarinos se han constituido como el núcleo central del flujo de información en el mundo.

En el mapa 1, se pueden observar los mapas submarinos existentes y los proyectados hasta el año 2023. De acuerdo a informes presentados por Equinix, el índice anual de interconexión global GXI, se pronostica que América Latina será la región de mayor expansión de capacidad de ancho de banda para interconexión a nivel mundial para el período 2019-2023. Esta circunstancia se encuentra relacionada a varios cables submarinos proyectados para dicho periodo (Ellalink, SPSC, Gignet-1 y el Caribbean Express). La creciente demanda de ancho de banda conlleva a la necesidad infraestructural de cables submarinos, muchos

de ellos fabricados y operados por empresas privadas (relacionadas a infraestructura de las telecomunicaciones).



Mapa 1: Cables Submarinos. Fuente: Submarine Cable Map (actualizado al 7 de abril 2021)

A pesar que los proveedores de estas infraestructuras son principalmente actores no estatales, el servicio provisto resulta estratégico para las naciones. Esto conlleva a pensar el valor, no solamente económico, sino también político de estos cables y las tecnologías relacionadas. Es por ello, que una política de ciberdefensa nacional y regional debe contemplar aspectos físicos además de los virtuales, es decir, los instrumentos de ciberdefensa deben contemplar la multidimensionalidad del dominio ciberespacial.

Hacia una Política de Ciberdefensa Nacional y Regional

Pensar la relación entre las infraestructuras críticas, su vínculo con el ciberespacio y sus vulnerabilidades implica una mirada amplia de la defensa nacional. Casos como los ciberataques en las centrales eléctricas de Ucrania en el 2015 o el ocurrido a principios de abril 2021 en el complejo nuclear de Natanz en Irán, ponen de manifiesto la predominancia del dominio ciberespacial en la lógica de la conflictividad del siglo XXI.

Al mismo tiempo, la expansión del ciberespacio en las múltiples esferas de la vida humana ha reforzado el debate en torno a la soberanía y su relación con la interdependencia. El mundo cibernético parece volver a poner en jaque la capacidad del Estado para controlar aquello que sucede en su territorio y que vuelve dificultoso el control sobre las fronteras. Más aún, considerando los argumentos de Farrell y Newman (2016) la globalización y la interdependencia han sido mecanismos utilizados en detrimento de la estabilidad y la seguridad global. Incluso, muchos de los efectos de las nuevas tecnologías sobre la salud de los seres humanos se encuentran en discusión habiéndose identificado una amplia gama de patologías mentales como la adicción a los videos juegos (Smith, Hummer y Hulvershorn, 2015).

Al no existir consensos en torno a la definición del ciberespacio y al haber una amplia gama de riesgos y amenazas que varían según cada nación, tampoco existen acuerdos respecto a la definición de soberanía en el ciberespacio. Si agregamos, además, la dinámica de la interdependencia compleja y su respectiva armamentización, y el desarrollo tecnológico, los desafíos políticos se complejizan.

El ciberespacio con su naturaleza dual, real y virtual, asentado sobre recursos tecnológicos que se encuentran a la vez, dentro y fuera de las fronteras de un Estado, que recorre un mundo interconectado, donde de un mismo flujo de información se nutren personas de todo el mundo, pese a sus diferentes culturas e idiosincrasias, plantea serios desafíos a la categoría de soberanía nacional y regional, tal cual la conocemos. En esta nueva era, caracterizada por la aceleración del cambio, la rapidez de las comunicaciones y del dominio cibernético, la soberanía de otros influye en la propia. La capacidad de ejercicio de soberanía en el mundo contemporáneo requiere de planificación estratégica y del desarrollo de infraestructura e instrumentos que permitan un correcto ejercicio de ella. Considerando, además, que muchas de estas infraestructuras construyen monopolios naturales compartidos por países de la misma región.

Sin duda el desarrollo científico-tecnológico e industrial será una de las principales aristas de poder, soberanía y crecimiento económico de las próximas décadas. La pregunta que queda por hacerse es: ¿qué

harán los países latinoamericanos al respecto?

NOTAS

1. Es muy común identificar a estos procesos con el nombre de Revolución Industrial 4.0 y Revolución Industrial 5.0. Términos acuñados por Klaus Schawb fundador del Foro Económico Mundial.

2. No es el primer ciberataque que recibe el complejo nuclear Natanz. En el año 2010 fue atacado por el Malaware Stuxnet, el cual se ha estudiado en profundidad en la última década.

REFERENCIAS BIBLIOGRAFICAS

Bloomberg (2021). Peter Thiel suggests Bitcoin may be 'a Chinese financial weapon against the U.S.' en *Fortune:* https://fortune.com/2021/04/07/peter-thiel-bitcoin-chinese-financial-weapon/.

Farrell, H. y Newman, A. (Summer 2019). "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," en *International Security*, Vol. 44, No. 1, pp. 42–79.

Fidler, D. (2021) "America's Place in Cyberspace: The Biden Administration's Cyber Strategy Takes Shape" en *Council on Foreign Relations.* https://www.cfr.org/blog/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape.

Gastaldi, S. y Ocón, A.L. (2019). "Ciberespacio y Defensa Nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía", en *Defensa Nacional*, No2, UNDEF, pp. 88-109.

Gastaldi, S. y Ocón, A.L. (Coord.) (2021). *Ciberdefensa: Claves para Pensar una Estrategia de Soberanía Nacional*. Taeda.

Koppel, T. (2015). "Where is America's cyberdefense plan?" En *The Washington Post:* https://www.washingtonpost.com/opinions/lets-talk-about-a-cyberdefense-plan/2015/10/30/efb19060-7cd7-11e5-b575-

d8dcfedb4ea1_story.html

Libicki, M. (2016). *Cyberspace in Peace and War*. Naval Institute Press.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Nye, J. (2010). *Cyber Power*. Belfer Center for Science and International Affairs. Harvard Kennedy School.

Ocón, A.L. (2021). "Abracadabra y la Biblioteca de Babel: Una aproximación geopolítica a la espacialidad del ciberespacio". En Gastaldí y Ocón *Ciberdefensa: Claves para pensar una estrategia de soberanía nacional*. Taeda.

Ocón, A.L. (2019). Democracia y Big Data: Incertidumbre y desafíos contemporáneos a la gobernabilidad, la transparencia y la Defensa Nacional en Defensa Nacional. En *Defensa Nacional*, UNDEF, pp. 32-55.

Singer, P.W. y Brooking, E.T. (2018). *Likewar: the weaponization of social media*. Houghton Mifflin Harcourt.

Sheldon, J. B. (2015). "The Rise of Cyberpower". En Baylis, John, James J. Wirtz, and Colin S. Gray (ed.) *Strategy in the Contemporary World: An Introduction to Strategic Studies (5th edn)*, pp. 282-298.

Smith, K.L., Hummer, T.A. y Hulvershorn (2015). "L.A. Pathological Video Gaming and Its Relationship to Substance Use Disorders". En *Curr Addict Rep* 2, 302–309.

Starosielski, N. (2015). *The Undersea Network (Sign, Storage, Transmission)*. Duke University Press.