(Ciber)Industria y Defensa: Un Aporte para el diseño de políticas de desarrollo frente al riesgo geopolítico en el Siglo XXI

Leandro Ocón*

Resumen: El artículo propone un análisis cualitativo descriptivo de las tendencias para la elaboración e implementación de política industrial en los albores del siglo XXI. Se destaca particularmente la problemática de dar respuesta a los escenarios geopolíticos que proponen las nuevas tecnologías de la comunicación y la información (TIC) y el ascendente grado de tensión y conflicto del sistema internacional. De esta forma, se presenta el concepto de política (ciber)industrial para abordar la particular relevancia que han tomado los instrumentos de desarrollo en el ciberespacio, considerando la tecnología como parte de un escenario geopolítico de riesgo. En este sentido, las dinámicas geopolíticas y las estrategias nacionales de ciberdefensa y ciberseguridad de los países más desarrollados han estado en sintonía con las políticas (ciber)industriales. Desde la perspectiva señalada, se intenta contribuir a un vacío académico que yace en el estudio del vínculo entre los modelos de desarrollo y las estrategias de defensa o seguridad nacional, considerando el rol de la geopolítica.

Palabras clave*:* geopolítica, industria, ciberespacio, desarrollo, tecnología

Abstract: The article proposes a qualitative descriptive analysis of the trends in the elaboration and implementation of industrial policy at the dawn of the 21st century. Emphasis is placed on the issues surrounding new communication and information technologies (ICT) and the geopolitics of cyberspace. In this way, the concept of (cyber)industrial policy is presented to address the particular relevance that development instruments in cyberspace have taken on, considering technology as part of a geopolitical risk scenario. In this sense, the geopolitical dynamics and national cyber defense and cybersecurity strategies of the most developed countries have been in tune with (cyber)industrial policies. From the aforementioned perspective, an attempt is made to contribute to an academic gap that lies in the study of the link between development models and national defense/security strategies considering the role of geopolitics.

Keywords: Geopolitics, industry, cyberspace, development, technology.

Recibido: 4 de noviembre del 2022. **Aceptado**: 16 de diciembre del 2022. **Publicado**: 29 de diciembre de 2022

* Licenciado en Ciencia Política (UdeSA), Magister en Estrategia y Geopolítica (ESG). Doctorando en Ciencia Política (UTDT). Investigador y docente en la Escuela Superior de Guerra del Ejército y en la Universidad de Champagnat. Editor y co-autor junto a Sol Gastaldi de "Ciberdefensa: Claves para Pensar una Estrategia de Soberanía Nacional" (2020), Compilador y co-autor junto a Aureliano da Ponte de "Industria y Defensa: Economía Política, Pensamiento Estratégico y Autonomía Tecnológica" (2016) y autor de "Educación, Conocimiento y Poder: debates lógico-epistémicos y enfoques alternativos respecto de la naturaleza humana" (2017). Autor en revistas académicas y de artículos de opinión en Diario Perfil, Ámbito y Revista DEF. Director de la Laboratorio de Planeamiento Estratégico "Cisne Negro". Conferencista y divulgador en temas referidos a guerra, tecnología, geopolítica y economía política. Leandro.ocon@gmail.com

Introducción

El presente artículo propone hacer un análisis cualitativo de las principales tendencias en la planificación, elaboración e implementación de política (ciber)industrial para la construcción de esferas de influencia y de ejercicio de poder en el ámbito ciberespacial, considerando la combinación de elementos militares y civiles. Es decir, una porción de la construcción del poder y de instrumentos de desarrollo de las naciones tiene como punto de partida una concepción geoestratégica del ciberespacio.

En este sentido, al referirnos a política (ciber)industrial, se considera un tipo específico de política industrial que contempla el aspecto transversal y multidimensional del ciberespacio (infraestructura, lógica-digital y cognitiva), además de la dualidad en materia tecnológica de las esferas civiles y militares. A saber, la política (ciber)industrial es una política industrial que aborda específicamente el sector ciberespacial -la ciberindustria- en tanto dimensión física como virtual, y que opera en una dimensión de riesgo geopolítico.

El sector ciberespacial o la ciberindustria es aquella destinada a la producción de las llamadas Tecnologías de la Información y Comunicación (TIC), *big data*, internet de las cosas (IoT), inteligencia artificial o cualquier otro tipo de tecnología, instrumento o herramienta que construye, obtiene, transmite, procesa, analiza o almacena datos de manera digital.

El principal objetivo del artículo es realizar una contribución al estudio de la política industrial desarrollada por Andreoni y Chang (2019) a partir de nueva evidencia que colabora con llenar un vacío académico con respecto al rol de las estrategias de defensa y seguridad nacionales. Considerando los aportes de Khan *et al.* (2022), la geopolítica juega un rol fundamental en la definición de la política industrial, así como en los cambios en el sistema internacional. Dicho esto, existe una relación insuficientemente explorada desde la economía política entre la política industrial y la defensa nacional.

Al propósito mencionado se le agrega la continuidad de una agenda de investigación en lo que respecta a la (geo)economía política y su vínculo con trayectorias de poder internacional. Específicamente, existe un vacío académico en torno a la relación entre el ciberespacio, el poder y el desarrollo industrial. Muchos autores contemporáneos, tales como Sheldon (2015) o Libicki (2016), analizan la construcción del poder en el ciberespacio (o ciberpoder), otorgando relevancia a la cuestión estratégica y su impacto en la práctica de los conflictos contemporáneos, pero poco profundizan en las capacidades industriales que las antenceden.

De forma cualitativa y descriptiva, el trabajo se organizará en cuatro apartados. En el primero de ellos, de forma introductoria, se hará una breve descripción del riesgo geopolítico en el ámbito de la tecnología y el ciberespacio de los últimos años, con el fin de echar luz en un proceso que se encuentra en continuo cambio. En el segundo acápite, se abordarán aspectos teóricos del desarrollo y de la composición geopolítica del ciberespacio desde una revisión de la bibliografía reciente. Se tendrá en consideración la dualidad civil-militar de las tecnologías orientadas al ciberespacio y algunos ejemplos de construcción de capacidades en base a las TIC. En la tercera sección, se analizarán el tipo de política (ciber)industrial que diversos países y entidades internacionales han elaborado e implementando con el fin de construir capacidades ciberespaciales. Finalmente, en el cuarto y último apartado se realizarán algunas reflexiones finales.

En síntesis, el trabajo se propone contribuir al debate existente en torno al vínculo entre modelo de desarrollo y estrategia de defensa de los Estados en el siglo XXI. Desde una perspectiva geopolítica analizaremos qué rol juega el Estado en el desarrollo tecnológico, cuáles son las nuevas orientaciones de la política industrial y cuál es la relación que se observa entre la defensa nacional, la industria y el ciberespacio.

El riesgo geopolítico

Desde el año 2018 se registra un aumento notable de la preocupación de los Gobiernos de distintos países por las innovaciones tecnológicas. Se observa un aumento de regulaciones y restricciones a la inversión de empresas extranjeras en el sector TIC. No es que la desconfianza sea algo nuevo, pero tal como lo demuestra el World Investment Report (UNCTAD en Aggarwal y Reddie, 2018), la tendencia general de los países desarrollados ha sido un mayor involucramiento del Estado en materia de tecnologías estratégicas, particularmente en torno a las TIC.

El mismo año que Donald Trump comienza la llamada "guerra comercial" con China (Fajgelbaum y Khandelwal, 2022), comenzó la competencia geopolítica tecnológica denominada como "carrera 5G", que no solamente anunciaba un auge de rivalidad entre empresas orientadas a la tecnología de las telecomunicaciones, sino también entre naciones, como protagonistas del impulso y el control tecnológico. La carrera del 5G, es uno de los tantos casos que reflejan el aumento de tensiones geopolíticas en el ámbito tecnológico por el ascenso de potencias económicas, tecnológicas y militares que compiten con Estados Unidos, generando lo que muchos autores han identificado como **riesgo geopolítico**.

La pandemia de COVID-19 tuvo un notable impacto en la geopolítica de la tecnología. Más que generar un terreno de cooperación internacional, los ámbitos de soberanía fueron aumentando en conjunto con el gasto militar, sumado a la necesidad de controlar y supervisar las nuevas tecnologías emergentes, las plataformas digitales y las infraestructuras críticas del ciberespacio. Al mismo tiempo, en el ámbito militar ya se identifica al ciberespacio como un nuevo dominio donde se ejecutan acciones específicas. Es decir, existe una nueva "espacialidad", que se ha constituido como una de las principales agendas estatales de las últimas décadas y que surge de la interacción entre la información, los seres humanos y las tecnologías (Gastaldi y Ocón, 2020).

A principio de octubre 2022 la administración de Biden presentó la Declaración de Derechos de Inteligencia Artificial (IA) y a comienzos de diciembre del 2022 el Consejo de la Unión Europea (CUE) comunicó la implementación del Acta de Inteligencia Artificial con el fin de proteger y asegurar los intereses europeos frente a dicha tecnología (CUE, 2022). Días más tarde, Putin declaró organización terrorista a Meta, la empresa que es propietaria de Facebook, Instagram, WhatsApp, entre otras plataformas virtuales (Duffy, 2022). Mientras tanto, la preocupación por el crecimiento de la red social TikTok aumentó en la Unión Europea, en Australia y en el Reino Unido, estando ya bloqueada en India desde el 2020.

Abundan ejemplos del auge del rol del Estado en materia tecnológica. Es posible observar que el ciberespacio se encuentra atravesado por relaciones de poder, y que el control o dominio de la información y la infraestructura críticas en torno al ciberespacio cumplen

un papel fundamental en la dinámica geopolítica contemporánea. "El desafío entonces pareciera ser cómo ganar autonomía –y soberanía– frente a la dependencia" (Gastaldi y Ocón, 2019, p. 105).

En los últimos años, en lo que respecta a la relevancia de las nuevas tecnologías militares y civiles de la información, es destacable la influencia de las TIC en materia de elaboración e implementación de política, estrategia y doctrinas. Más allá de la relevancia socioeconómica y la mirada política de la globalización o la convergencia tecno-política, en la actualidad, este es un ámbito de disputa de poder geopolítico.

Si bien el ciberespacio es uno de los principales ámbitos económicos y se observa en él un gran crecimiento en las últimas décadas, también cabe destacar lo que ha crecido el ámbito de defensa y seguridad de las naciones. Son dos caras de una misma moneda: el crecimiento económico y de la defensa nacional dentro de un mismo esquema estratégico. En muchos casos, ha sido la estrategia de desarrollo de defensa y seguridad nacional la que ha impulsado la adopción de innovaciones tecnológicas que hoy gozan de un gran estatus comercial.

En sintonía con la tendencia geopolítica contemporánea, se sostiene que un enfoque de defensa disociado de la política industrial ignora la importancia de los aspectos geoestratégicos de la competencia entre las grandes potencias. En particular, hemos visto a Estados Unidos, Rusia, China y los países europeos realizar inversiones relacionadas con tecnologías emergentes críticas en sus propios mercados y utilizar herramientas como la política industrial y la nueva legislación diseñada para impactar en la inversión transfronteriza, en las fusiones y adquisiciones de tecnologías para las empresas (Comisión Económica y Social de las Naciones Unidas para Asia y el Pacífico -UNESCAP-, 2018).

En definitiva, y tal como señalan Aggarwal y Reddie (2018), nos encontramos frente a una nueva era de política industrial que busca de forma simultánea y armónica combinar dimensiones de defensa nacional, desarrollo económico e innovación tecnológica. Tal como señalan los autores, las principales economías (Estados Unidos, China, Rusia, India, Francia, Alemania, Japón, etc.), en la última década, han elaborado políticas industriales orientadas al ciberespacio con el fin de resguardar su soberanía tecnológica, proteger infraestructura crítica y generar desarrollo tecnológico y económico.
Es decir, se observa que la nueva forma de construcción de poder geopolítico es a partir de la construcción de capacidades económicas, militares y tecnológicas sustentadas en lo que podría denominarse política (ciber)industrial. Dichas políticas públicas se constituyen, principalmente, desde un enfoque estratégico con una puesta multidimensional en el desarrollo económico, la reducción de dependencia y la construcción de poder propio o colectivo.

La política (ciber)industrial contemporánea revela varias cuestiones académicas y políticas en lo que respecta a los debates de economía política contemporánea. En primer lugar, la dualidad civil-militar que presentan las TIC. En segundo lugar, la manera en que la política industrial y científica-tecnológica representa una cuestión no solamente económica, sino también relacionada a la seguridad y la defensa nacional. En tercer lugar, se observa cómo la política orientada al ciberespacio se sustenta en infraestructura física y virtual. Finalmente, en cuarto lugar y desde una perspectiva global, la cuestión de la

tecnología es una dimensión fundamental de las problemáticas geopolíticas contemporáneas.

En síntesis, si consideramos las estrategias nacionales de defensa o seguridad de Rusia, India, China, Estados Unidos, Reino Unido y Francia, la construcción de sus capacidades, la promoción de su crecimiento económico y la ampliación de su poder en el ciberespacio observamos que se trata de uno de los principales objetivos estratégicos hacia 2030. Lo que años atrás había surgido como un espacio de cooperación, libertad e interacción, hoy se presenta como una dimensión de competencia, control y soberanía. Diversos estudios han demostrado que el ciberespacio expone a las naciones a tal punto que quedan vulnerados los sistemas electorales, las infraestructuras críticas, la economía o la información estratégica que resulta vital para los gobiernos y los ciudadanos (Nye, 2010, 2016; Libicki, 2016; Gastaldi y Ocón, 2019). Por lo tanto, más allá de los esfuerzos que se puedan realizar a nivel individual, el ciberespacio demanda una política que contemple múltiples dimensiones en simultáneo.

Tal como señalan Khan *et al.* (2022), existe una profunda relación entre el riesgo geopolítico y la tecnología. El poder de las naciones se encuentra asociado a la demanda incremental de desarrollo tecnológico. En este sentido, los albores del siglo XXI se presentan con una acelerada expansión ciberespacial, el desafío de la convergencia digital, las TIC, 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. Todos estos factores repercuten directamente en el desarrollo y el poder de las naciones.

Geopolítica del ciberespacio

Como se mencionó anteriormente, el ciberespacio se ha constituido como uno de los principales "espacios" de interacción entre seres humanos, para la cooperación, la competencia e, incluso, para el conflicto. Dentro de esta lógica, se presenta como un dominio donde existen intereses individuales, nacionales, regionales y globales en una compleja dinámica.

El ciberespacio, como espacio geopolítico, se caracteriza por su complejidad y transversalidad. Ahora bien, ¿cómo se define el ciberespacio? Uno de los principales desafíos que se presentan a la hora de abordarlo es comprender qué es y cómo funciona. Si bien existen múltiples definiciones del término, se propone utilizar la siguiente, que considera los aportes de Libicki (2016) y Ocón (2020, 2021): el ciberespacio es un espacio cognitivo transversal constituido en base a una dimensión física y una lógica. Dicha espacialidad se construye a partir del lenguaje, contempla elementos técnico-físicos y cognitivos.

El ciberespacio como tal, se caracteriza por una **transversalidad** que involucra múltiples dimensiones o capas. El ciberespacio es un espacio de relaciones cognitivas mediadas por dispositivos técnicos y por mecanismos cognitivos de vinculación basados en el lenguaje que transcurre multidimensionalmente (Libicki, 2016; Gastaldi y Ocón, 2020). Dichas capas se integran verticalmente y se ordenan de forma tal que cada una hace posible la existencia de la subsiguiente.

Lo aquí propuesto pretende visibilizar la dualidad física y cognitiva del ciberespacio y cómo la energía se transforma en información. Por un lado, se observan todos los dispositivos duros o *hardware*, tales como rúteres, cables, satélites, etc. Por otro lado, el lenguaje constituye una faceta "semántica" que se entiende como la dimensión en la cual la información adquiere significado para los seres humanos. El proceso de transformación de energía en información es lo que se constituye como un fenómeno transversal. Dentro de esta lógica, se puede afirmar que existen cuatro "capas": la físico-geográfica, la de la infraestructura física, la dimensión lógica-digital y, finalmente, la cognitiva.

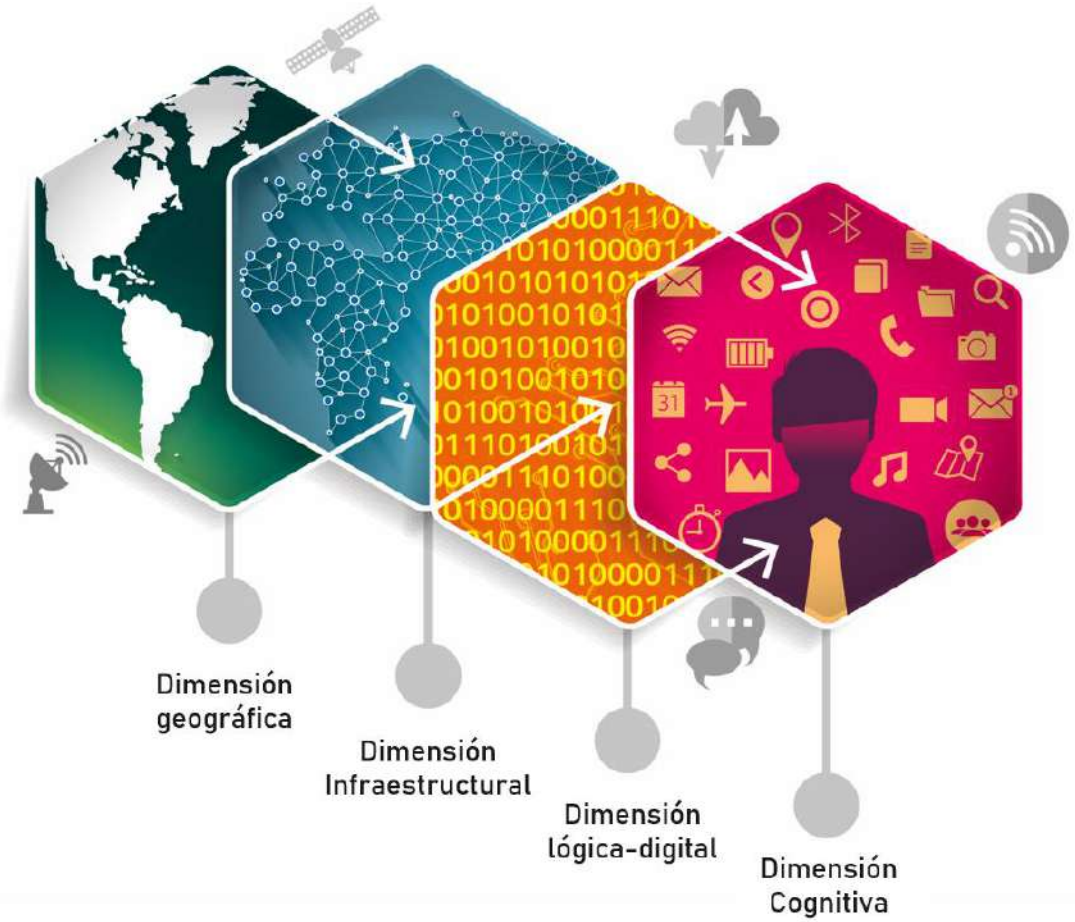

Figura 1: Las dimensiones transversalidad del ciberespacio
Fuente: elaboración propia de acuerdo con los aportes de Gastaldi y Ocón (2020)[1]

En la figura 1 se observan las dimensiones que componen el ciberespacio y cómo se estructura la transversalidad. Esta forma de abordaje responde a los diversos aportes teóricos realizados por la Organización del Tratado del Atlántico Norte (OTAN, 2009), Libicki (2009), Grant (2014), Nissen (2015), Strate (2018) y Gastaldi y Ocón (2020).

La **dimensión geográfica** es el mundo físico con sus propias características naturales (océanos, ríos, bosques o montañas) que funcionan como determinantes en la vida humana. Sobre este mundo "natural", el hombre construye infraestructura física que da origen a la segunda capa o dimensión.

[1] En la versión de Gastaldi y Ocón (2021) el ciberespacio es considerado la última capa, la que corresponde a la dimensión cognitiva en la Figura 1. Es decir, en el presente trabajo, el ciberespacio es el conjunto de las 4 capas de forma transversal.

La **infraestructura física** (del ciberespacio) no solamente incluye a los dispositivos técnicos que dan origen a internet, sino que también abarca toda la estructura humana (instituciones formales e informales, normas, organizaciones, etc.) sujeta a una metamorfosis tecnológica anclada a la digitalización, que implica la administración e interconexión con redes informáticas. También se encuentra aquí lo que se identifica como **infraestructuras críticas**, es decir, obras públicas, instituciones u organizaciones que forman parte del ecosistema infraestructural y que, sin ser estructurantes del ciberespacio, juegan un papel estratégico para el funcionamiento de los países (por ejemplo, una planta de producción de energía nuclear o el sistema hospitalario) (Miranzo y Del Río, 2014). Esta es una de las principales preocupaciones a la hora elaborar planes para la ciberdefensa.

Por ejemplo, un caso interesante es el de Argentina: la Decisión Administrativa 641/2021 presenta la diferencia entre infraestructuras críticas e infraestructuras críticas de la información. Las primeras son:

> Aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente y las infraestructuras críticas de la información[2].

Por su parte, las infraestructuras críticas de la información son "aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas"[3].

Ahora bien, en lo que respecta a la capa infraestructural del ciberespacio se identifican, por ejemplo, los cableados terrestres y submarinos, los espacios de almacenamiento y de procesamiento de la información. La construcción de los medios para la circulación de información y su capacidad de permanecer en un espacio físico de forma lógico-digital se constituye en una nueva capa, donde transcurren los procesos de (de)codificación de energía en lenguaje binario. Dicha capa es la que conecta transversalmente el ciberespacio con el mundo físico, es decir, mantiene relación con el mundo físico, pero al mismo tiempo se separa de él por medio del mecanismo de transformación del lenguaje (Gastaldi y Ocón, 2020).

A partir de las posibilidades tecnológicas que permiten estos **mecanismos lógico-digitales**, se estructura una nueva dimensión que posee una naturaleza espacial propia. Aquí se articula la relación entre seres humanos, y entre estos y la infraestructura física, por medio de una **transformación lingüística y cognitiva.** Se originan núcleos puramente digitales de interacción, comercio, de ocio, de aprendizaje, entre otras cosas.

Este proceso ha sido continuo a partir del acceso masivo a dispositivos tecnológicos (como *smartphones* o infraestructura digital) y la explosión de datos permitió la creación del *big data* y su integración con el IoT. Ahora bien, el avance propio de la tecnología y su transversalidad ciberespacial ha ocupado un lugar central en el desarrollo de las últimas

[2] Decisión Administrativa 641/2021 de 2021. Requisitos mínimos de seguridad de la información de la información para organismos. Preámbulo. 28 de junio de 2021. BO nro. 34688.
[3] Decisión Administrativa 641/2021 de 2021. Requisitos mínimos de seguridad de la información de la información para organismos. Preámbulo. 28 de junio de 2021. BO nro. 34688.

décadas. Dicho desarrollo posee, además, una relación intrínseca con incidentes informáticos debido al surgimiento de nuevas formas de ingeniería social asociadas al crimen o la capacidad de influencia política a gran escala (Libicki, 2016; Gastaldi y Ocón, 2020). De esta manera, surge la profunda relación entre el desarrollo del ciberespacio y la defensa nacional.

En este sentido, así como el desarrollo económico industrial de las naciones se encuentra asociado a su poder militar y a su capacidad de ejercer la seguridad nacional, el ciberespacio se encuentra unido a la capacidad ciber(industrial). En la medida que los Estados, las empresas y la sociedad civil en su conjunto, aumentan los grados de acción e interacción en el ciberespacio, nuevas tecnologías nacen y acompañan estos desafíos estratégicos.

Este continuo desarrollo del ciberespacio y su actual expansión se suma a la dinámica tecno-política asociada al poder militar de las naciones. Por ejemplo, los sistemas de armas se complejizan -con el fin de aumentar sus capacidades- y este desarrollo se encuentra acompañado del surgimiento de nuevas vulnerabilidades que demandan, en consecuencia, respuestas (soluciones) tecnológicas nuevas. A cada nuevo desarrollo le corresponde una nueva forma de respuesta tecnológica.

Nos encontramos en una esfera híbrida dónde el *hard power* se combina con el *soft power*. Esta hibridación genera la necesidad de abordar el ciberespacio como un ecosistema compuesto por *hardware* y *software*, que se articulan entre sí, a partir de una compleja dinámica tecnológica. Este fenómeno pone de manifiesto la creciente necesidad de políticas públicas y de capacidad productiva con un trasfondo técnico sustancial en un ámbito en constante cambio. Hay una tecno-política/industria asociada directamente con el poder en el ciberespacio.

El ciberespacio es, en definitiva, una construcción humana que se estructura en base a industria y tecnología que se orientan a la producción, almacenamiento, transmisión y uso de datos. Los datos cobran cada vez mayor relevancia estratégica al tiempo que poseen un rol central en el funcionamiento de las sociedades, las economías, el instrumento militar y/o las instituciones humanas.

En general, la forma en la que se han desarrollado los mercados en materia de TIC, ciberdefensa y *software* ha tenido al Estado como protagonista. Por ejemplo, Estados Unidos, Francia o Corea del Sur, son algunos casos paradigmáticos que han construido sus capacidades soberanas a partir de políticas industriales orientadas específicamente a las capacidades productivas (Lewis, 2016). Evidencia de ello es *Loi de Programmation Militaire-LPM 2014–2019* francés, la Agencia de Proyectos de Investigación Avanzados de Defensa (en adelante, DARPA) en Estados Unidos, o los *chaebol* de Corea del Sur.

La integración científico-tecnológica del ámbito civil y militar también es visible en las estrategias de desarrollo. Muchos de los grandes esfuerzos estratégicos recientes de los países centrales han buscado reforzar las capacidades multidominio del ámbito militar. Si consideramos la complejidad de las dinámicas convencionales y no convencionales de los actores (estatales y no estatales), sumado a las nuevas tecnologías y a la expansión del ciberespacio, se puede ver que se ha gestado una necesidad de respuesta que motiva el desarrollo tecnológico en los sectores productivos vinculados al ciberespacio. La decisión política estratégica orientada a la innovación en materia de TIC, IoT, ciberdefensa,

radares, satélites ópticos, inteligencia artificial, ciencias de datos, etc.; se convierte en el principal elemento que impulsa el desarrollo productivo en el ámbito de la defensa y la seguridad nacional.

Las arquitecturas de la información, especialmente en materia de ciberdefensa, no solamente han estado centradas en la protección de infraestructuras críticas, sino también en la capacidad de acción en los escenarios operativos. En particular, se destaca la importancia de C4ISR (comando, control, comunicaciones, computación, inteligencia, vigilancia, reconocimiento) (Sowell, 2006), que no es otra cosa que una forma integrada de obtener información y procesar la toma de decisiones en forma de acciones coordinadas frente a escenarios operativos que demandan respuestas rápidas.

De esta manera, las capacidades de los Estados se encuentran asociadas a la creación de arquitecturas de *hardware*, *firmware* y *software* específicos que articulen la complejidad de los fenómenos y que respondan con sistemas tecnológicos que fortalezcan el ejercicio de la soberanía y la protección de la ciudadanía. En este sentido, y más allá de las instituciones, el ciberespacio es una dimensión o dominio tecno-político dual y transversal.

En síntesis, las TIC no se encuentran disociadas de la base industrial de los países que las originan. Más aún, como tecnologías duales y estratégicas se encuentran intrínsecamente vinculadas a la política de ciberdefensa, de seguridad y a la política industrial como un espacio de ejercicio de soberanía tecnológica y desarrollo económico.

La política (ciber)industrial en el siglo XXI

De acuerdo a Aggarwal y Reddie (2019) existen cinco formas en las cuales la política industrial (en los países desarrollados) se ha orientado en materia de generación de capacidades en el ciberespacio: a) creación de mercados, b) facilitación de mercados, c) modificación de mercado, d) proscripción de mercado, y e) sustitución de mercado.
En primer lugar, el Estado como creador de mercados, es aquel que se convierte en el principal cliente de bienes y servicios. Como se mencionó anteriormente, algunos ejemplos como Francia, Estados Unidos, China y Corea del Sur, ponen de manifiesto que el Estado se posiciona como el principal cliente de empresas nacientes o ya constituidas para facilitar el desarrollo de sectores estratégicos y asegurarse la continuidad de organizaciones productivas.

En segundo lugar, las políticas de facilitación de mercados buscan reducir los costos de transacción, mejorar los mecanismos de promoción en determinadas áreas o en determinado sector y/o asumir costos -desde el Estado- para mejorar el margen de acción de las empresas. Ejemplos de ello son las aceleradoras, como el Acelerador de Tecnología de Seguridad Nacional (NSTXL) dependiente de la Unidad de Innovación del Departamento de Defensa norteamericano, o los subsidios e incentivos fiscales existentes en Japón, Finlandia, Israel (Lewis, 2016), entre otros casos.

En tercer lugar, siguiendo con el desarrollo planteado por los autores, las políticas de modificación de mercado utilizan regulaciones para cambiar las conductas de los sujetos, el medio o los términos del intercambio, con el objetivo de generar resultados diferentes de los que el mercado tiende a producir. Recientemente, la Comisión Europea ha desarrollado una serie de reglas con respecto al uso de la información, estandarización, y

certificación similar a la OTAN o a la de Estados Unidos. Algunos países aplican políticas proteccionistas sobre todo ante el accionar de actores externos que intentan ocupar segmentos estratégicos y generar dependencia tecnológica, en ocasiones, por medio de mecanismos tipo *dumping*.

En cuarto lugar, la forma más común mediante la cual los gobiernos proscriben formas de mercado es la prohibición. En general, ocurre por medio de controles de exportación o normas de contratación. En ocasiones, las prohibiciones se emiten directamente desde el Estado, como la Ley de "Control de Exportación de Armas" de Estados Unidos; o través de vetos específicos, como opera la *UK Strategic Export Control List* del Reino Unido.

Para finalizar con la clasificación propuesta por Aggarwal y Reddie (2019), la sustitución de mercado como política industrial, implica la creación de mercados por parte del Estado allí donde no existe la iniciativa del sector privado. Es decir, la sustitución ocurre cuando el Estado se transforma de manera activa en inversor o impulsor de dicho sector, por ejemplo, el caso de In-Q-Tel, una entidad de capital de riesgo sin fines de lucro vinculada con la comunidad de inteligencia de Estados Unidos. En el 2015, la CIA (Agencia Central de Inteligencia) puso en funcionamiento la Dirección de Innovación Digital, encargada de identificar sectores estratégicos productivos en tecnologías emergentes que pueden ser apoyadas por capitales nacionales.

En síntesis, la tendencia de países más desarrollados se ha orientado a la promoción de políticas (ciber)industriales vinculadas con la innovación y creación de tecnologías estratégicas tanto para la esfera civil como la militar. En este sentido, las políticas ciberespaciales han evidenciado una profunda relación entre el modelo de desarrollo y las estrategias de defensa (o de seguridad nacional). Tal como señala Timmers (2018) la estrategia de ciberseguridad de la Unión Europea (2017) consideraba impulsar una política industrial a nivel regional mediante una certificación de ciberseguridad que fortalezca la agencia de ciberseguridad de la Unión Europea (ENISA), promueva la creación del Centro de Competencia en Ciberseguridad de la UE (creado en 2021) y articule un enfoque común para el escrutinio de la inversión extranjera directa.

Para continuar con el análisis de los hechos que vinculan la geopolítica, la defensa y la industria (Ocón y Da Ponte, 2019; Khan *et al.*, 2022), el poder militar y el de la seguridad pública dependen de capacidades técnicas y operativas asociadas al instrumento disponible. Es decir, existen tecnologías específicas concomitantes al ciberespacio que se posicionan como estratégicas y son claves para la proyección de poder internacional. Más aún, autores como Khan *et al.* (2022) demuestran cómo el desarrollo tecnológico, desde principios del siglo XXI, estuvo impulsado por el riesgo geopolítico y consecuentemente, terminó por ser un componente más de riesgo entre potencias.

Dentro de esta lógica, tal como señalan Andreoni y Gregory (2013), la política industrial orientada a la producción de bienes y servicios todavía es relevante, a pesar de los preceptos que se poseían de la globalización y la interdependencia a fines del siglo XX. A la fecha, las naciones industrialmente desarrolladas siguen reteniendo en sus propios territorios las capacidades tecnológicas y productivas que consideran estratégicas.

Por ejemplo, la relación entre la geopolítica y la tecnología es un aspecto dual y estratégico, particularmente visible en la llamada "carrera del 5G". Básicamente, esta es

una competencia por el desarrollo, distribución y uso de tecnologías de quinta generación de telefonía móvil, que se presenta habitualmente como un ámbito de competencia entre Estados Unidos y China. Cabe destacar que la Unión Europea y Corea del Sur han realizado notables esfuerzos en definir su propia soberanía tecnológica y han generado algunos mecanismos alternativos a la tendencia bipolar en el sector (Da Ponte, León y Álvarez, 2022). Un ejemplo destacable de lo mencionado anteriormente se observa en la estrategia nacional de ciberseguridad impulsada en 2018 en Estados Unidos, donde se combinan objetivos de seguridad nacional con otros de promoción económica. Se observa un especial interés en el impulso de capacidades tecno-productivas de vanguardia. La estrategia incluye requisitos en las cadenas de valor de las compras públicas, definición de determinados estándares, control de fusiones y adquisiciones de tecnologías consideradas estratégicas, además del énfasis en la ciberseguridad para la protección de propiedad intelectual de innovaciones.

Por su parte, Brasil se encuentra entre los pocos Estados latinoamericanos que ha logrado realizar importantes avances en materia (ciber)industrial, motivado en gran parte, por la necesidad de asegurar su soberanía nacional y la posibilidad de ubicarse como un actor central en la región y en el mundo. En este sentido, tanto Leiva (2015) como Cruz Lobato (2017) han demostrado que el liderazgo brasileño ha sido sustancial para la elaboración de la arquitectura de ciberseguridad nacional y revela dos caras de la misma moneda: su avance como líder regional y, al mismo tiempo, una forma de construir dicho liderazgo (Gastaldi y Ocón, 2020).

En el Concepto Estratégico 2022 de la OTAN (OTAN, 2022) se presentan una serie de propuestas en torno a la promoción de la innovación y al aumento de las inversiones en empresas emergentes y disruptivas de tecnología, para mantener la interoperabilidad y la ventaja militar. El objetivo es gestar un trabajo conjunto y cooperativo entre los países miembros para adoptar e integrar nuevas tecnologías, vinculadas con el sector privado, que protejan los ecosistemas de innovación.
La atención de la OTAN en la política (ciber)industrial es particularmente visible en el foro de la Industria de la OTAN o en la Iniciativa OTAN 2030. En este sentido, hacia 2030, la política estratégica de la OTAN en materia de desarrollo productivo se canaliza a través del Acelerador de Innovación de Defensa civil-militar para el Atlántico Norte (DIANA). DIANA cumple la finalidad de promover la cooperación transatlántica en tecnologías críticas, la interoperabilidad y la innovación civil en búsqueda de conectar los sectores académicos con el sector civil, con particular atención en el sector privado. Como parte de la iniciativa DIANA, se creó el Fondo de Innovación de la OTAN.

DIANA tiene notables similitudes con DARPA, una de las agencias más importantes de Estados Unidos de Ciencia y Tecnología en la esfera del Departamento de Defensa. DARPA fue pionera en la creación del Internet, y hoy cuenta con un presupuesto anual aproximado de 3000 millones de dólares (DARPA, 2021).

La Unión Europea y la OTAN tienen múltiples espacios de cooperación en lo que respecta a políticas orientadas al desarrollo de capacidades en el ciberespacio (Röhrig y Smeaton, 2014). En un informe de la universidad de Berkley, Aggarwal y Reddie (2019) demuestran cómo el Estado ha jugado un rol fundamental en materia de industria de la ciberdefensa en países como Francia o Estados Unidos, no solamente con políticas públicas orientadas a corregir "fallas de mercado", sino como protagonista del desarrollo de tecnologías estratégicas. Vale la pena señalar que Francia se encuentra operando en

este sentido en múltiples dimensiones organizacionales, tanto a nivel nacional como a nivel de la Unión Europea y la OTAN.

Si se consideran los argumentos de Michael Kolton (2017) con respecto a la estrategia china de ciberdefensa, nos encontramos nuevamente con los conceptos claves de soberanía tecnología, capacidad militar y desarrollo económico. La postura estratégica de China no solamente ha conseguido cimentar un mecanismo de crecimiento propio, sino también se ha convertido en una herramienta de disputa contra Estados Unidos por la hegemonía.

El 16 de diciembre del 2015, Xi Jinping instó a la comunidad internacional a "respetar el derecho de los países individuales a elegir de forma independiente su propio camino de desarrollo cibernético y modelo de regulación cibernética y participar en la gobernanza internacional del ciberespacio en pie de igualdad" (en Kolton, 2017, p. 125)[4].

Tal como revela el autor, para el Estado chino, el ciberespacio (considerando su dualidad y transversalidad) es una dimensión central para lograr el "sueño chino" propuesto por Xi Jinping al tomar el control del Partido Comunista chino y, así, el liderazgo de la nación.

Reflexiones finales

El presente artículo no pretende ser de ninguna forma exhaustivo ni sistémico, sino un breve aporte descriptivo de las tendencias contemporáneas en política de desarrollo y de defensa. Se pone de manifiesto la existencia de un tipo de política (ciber)industrial que apuntala ambas esferas o dimensiones de forma simultánea, a partir de un abordaje geopolítico del ciberespacio.

Las dinámicas geopolíticas y las estrategias nacionales de los países desempeñan un papel fundamental en el tipo de política (ciber)industrial. En el escenario contemporáneo, la tensión multipolar se ve reflejada en el desarrollo de tecnologías estratégicas.

De acuerdo con los argumentos presentados, el abordaje del ciberespacio desde una perspectiva geopolítica permite echar luz a una cuestión fundamental: la construcción misma de las dinámicas espaciales en el ámbito cibernético depende de las capacidades industriales-tecnológicas de los países. Los países más desarrollados elaboran e implementan diversos tipos de políticas (ciber)industriales que les permiten construir y ejercer el (ciber)poder.

La construcción del ciberespacio, asociado al desarrollo tecno-económico de las naciones permitió, entre otras cosas, la rápida expansión de la actividad económica, social y política colaborando con el auge de la multipolaridad. Esta multipolaridad hoy se presenta como riesgo geopolítico.

Es claro que el contexto internacional ha ido modificándose a lo largo del tiempo y esto ha provocado diversos cambios en las visiones y en las respuestas de las naciones a la política industrial y científico-tecnológica. No obstante, cabe destacar la diversidad de instrumentos posibles que implementan los países desarrollados para generar innovación y autonomía local, y que pueden tomarse como ejemplo para nutrir las iniciativas de los

[4] [traducción propia]

países en vías de desarrollo. Se observan distintas categorías de políticas que son trasladables a la realidad de otras regiones que aún no comenzaron a estudiar en profundidad este fenómeno.

En este sentido, el presente artículo pretende ser un aporte al estudio de la política industrial en perspectiva histórica, considerando su relación con la geopolítica y las estrategias de seguridad y defensa nacional. A lo largo de los puntos desarrollados se ha presentado evidencia con el objetivo de demostrar aspectos fundamentales de la relación que existe entre el modelo de desarrollo y las políticas de defensa o seguridad nacional de los países más desarrollados.

De ninguna manera este es un trabajo de investigación acabado ni concluyente. En todo caso, propone una arista de investigación a partir de un enfoque específico (políticas industriales) para comprender una variable crucial en el desarrollo económico y militar de las naciones. La orientación de la política industrial permite observar las tendencias y prioridades estratégicas y cómo interactúan con los objetivos políticos de los Estados.

Al mismo tiempo, países de menores niveles de desarrollo pueden considerar las estrategias duales e integradas de otros países sin perder de vista que toda tecnología desarrollada responde a un interés (geo)político específico. Desde la perspectiva de la economía política comparada, se echa luz sobre los límites de teorías tales como las ventajas comparativas y libertad de mercado en lo que respecta a núcleos instrumentales estratégicos para el ejercicio de la soberanía.

En definitiva, tecnologías que no son estrictamente militares tienen un papel fundamental en lo que respecta al poder duro de las naciones. La relación entre el modelo de desarrollo y la estrategia de defensa nacional depende de una activa participación del Estado articulando la relación y los intereses del entramado productivo (público y privado) y los sectores orientados a la innovación y al desarrollo científico-tecnológico. El principal desafío yace en la capacidad de los estados de diseñar e implementar política pública que colabore con el multi objetivo de construir capacidades militares, económicas, científicas y comerciales en el ámbito ciberespacial.

El camino continúa, no solamente abre una agenda de investigación en sí misma, sino que permite la construcción categórica de modelos y estrategias acordes al escenario que plantea los albores del siglo XXI, caracterizado por la tensión, la competencia, el conflicto y las aspiraciones de hegemonía geo y tecnopolítica.

Bibliografía

Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) (2021). *Defense Advanced Research Projects Agency. Defense-Wide Justification Book Volume 1 of 5*. Defense Advanced Research Projects Agency.

Aggarwal, V. K. y Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: a framework for analysis. *Journal of Cyber Policy, 3 (3),* pp. 452-466.

Andreoni, A. y Chang, H. (2019). "The Political Economy of Industrial Policy: Structural Interdependencies, Policy Alignment and Conflict Management". *Structural Change and Economic Dynamics*, (48), pp. 136-150.

Andreoni, A. y Gregory, M. (2013). "Why and How Does Manufacturing Still Matter: Old Rationales, New Realities". *Revue d'économie industrielle*, 144, pp. 21-57.

Comisión Económica y Social de las Naciones Unidas para Asia y el Pacífico (UNESCAP) (2018). *Frontier Technologies for Sustainable development in Asia and the Pacific*. UNESCAP.

Consejo de la Unión Europea (2022) Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights. *Comunicado de Prensa* https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

Cruz Lobato, L. (2017). "La política brasileña de ciberseguridad como estrategia de liderazgo regional". *Revista Latinoamericana de Estudios de Seguridad*, 20 (1), pp. 16-30.

Da Ponte, A., León, G. y Álvarez, I. (2022). "Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach". *Telecomunications Policy*. 102459. 10.1016/j.telpol.2022.102459.

Decisión Administrativa 641/2021 de 2021. Requisitos mínimos de seguridad de la información de la información para organismos. Preámbulo. 28 de junio de 2021. BO nro. 34688.

Duffy, K. (2022) "Russia has added Meta to a list of 'extremist' and 'terrorist' organizations, a report says". *Business Insider* https://www.businessinsider.com/russia-adds-meta-list-extremist-terrorist-groups-facebook-zuckerberg-report-2022-10

Fajgelbaum, P. D. y Khandelwal, A. K. (2022). "The Economic Impacts of the US–China Trade War". *Annual Review of Economics, 14* (1), pp. 205-228.

Gastaldi, S. y Ocón, L. (2019). "Ciberespacio y Defensa Nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía". *Revista UNDEF*, 1 (2), pp. 88-108.

Gastaldi, S. y Ocón, L. (2020). *Ciberdefensa: Claves para pensar una estrategia de soberanía nacional.* Buenos Aires: Taeda.

Grant, T. J. (2014). "On the Military Geography of Cyberspace". En Liles, S. (eds.) *Proceedings, 9th International Conference on Cyber Warfare &* Security (pp.66-76). Thessaloniki: Purdue University.

Khan, K., Su, C., Umar, M. y Zhang, W. (2022). "Geopolitics of Technology: A New Battleground?" *Technological and Economic Development of Economy*, 2 (28), pp. 442–462.

Kolton, M. (2017). "Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence". *The Cyber Defense Review*, 2 (1), pp. 119-154.

Leiva, E. (2015). "Estrategias nacionales de ciberseguridad: estudio comparativo basado en enfoque top-down desde una visión global a una visión local", *Revista Latinoamericana de Ingeniería de Software,* 3 (4), pp. 161-176.

Lewis, J. A. (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad Panorama general de Estonia, Israel, República de Corea y Estados Unidos. *Banco Interamericano de Desarrollo,* IDB-DP-457.

Li, H., Yu, L. y He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management, 22* (1), pp. 1-6.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation.

Libicki, M. (2016). *Cyberspace in Peace and War*. Annapolis: Naval InstitutePress.

Miranzo, M. y Del Río, C. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers,* (35), pp. 339-352.

Mulligan, D. K. y Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus, 140* (4), 70-92.

National Research Council (2016). *C4ISR for Future Naval Strike Groups.* The National Academies Press.

Nissen, T. E. (2015). *The Weaponization of Social Media: Characteristics of Contemporary Conflicts.* Copenhagen: Royal Danish Defense College.

Nye, J. (2010). "El poder blando y la política exterior americana". *Relaciones Internacionales*, pp. 118-140.

Nye, J. (2016). "Deterrence and Dissuasion in Cyberspace". *International Security, 41* (3), pp. 44–71.

Ocón, L. (2021). Aportes Teóricos a la Geopolítica Regional del Ciberespacio. *Pensamiento Propio,* 53, pp. 241-250.

Ocón, L. y Da Ponte, A. (2016). *Industria y Defensa: Economía Política, Pensamiento Estratégico y Autonomía Tecnológica.* Buenos Aires: Editorial 1884.

Ocón, L. y Da Ponte, A. (2019). "Política Internacional y Defensa en el Siglo XXI: Entre la incertidumbre, la ciencia ficción y las nuevas dinámicas tecnológicas. *Relaciones Internacionales,* 28 (56), pp. 98–116.

Organización del Tratado del Atlántico Norte (OTAN) (2009). Allied Joint Doctrine For Information Operations Document (Ajp-3.10). OTAN. https://info.publicintelligence.net/NATO-IO.pdf.

Organización del Tratado del Atlántico Norte (OTAN) (2016). Warsaw Summit Communiqué issued by NATO Heads of State and Government. NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Organización del Tratado del Atlántico Norte (OTAN) (2022). Strategic Concept. OTAN.

Presidencia de los Estados Unidos de América (2018). National Cyber Strategy of the United States of America. Presidencia de los Estados Unidos de América.

Röhrig, W. y Smeation, R. (2014). "Cyber Security and Cyber Defence in the European Union: Opportunities, Synergies and Challenges*". Cyber Security Review, (1),* p. 25.

Sheldon, J. B. (2015). "The Rise of Cyberpower". En Baylis, J., Wirtz, J. J. y Gray, C. S. (ed.) *Strategy in the Contemporary World: An Introduction to Strategic Studies. 5ta. edición* (pp. 282-298). Oxford: Oxford University Press.

Sowell, K. (2006). The C4ISR Architecture Framework: History, Status, and Plans for Evolution. *Report MITRE Organization.*

Strate, L. (2018). "Eight Bits About Digital Communication". *Razón y Palabra, 22* (1_100), pp. 589-618.

Timmers, P. (2018). "The European Union's cybersecurity industrial policy". *Journal of Cyber Policy, 3 (3),* pp. 363-384.

World Economic Forum (2022). Global Cybersecurity Outlook 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf