Daniel Andrés Birchner 18/1/2025

INTRODUCCIÓN A UNA GEOPOLÍTICA DEL CIBERESPACIO

Hablar de ciberespacio supone, en primera instancia, referirse a un espacio virtual, intangible, en el que convergen interconexiones de información globales, sistemas informáticos y bases de datos. William Gibson popularizó el término en su novela cyberpunk *Neuromante*, de 1984, y definió al ciberespacio como una suerte de *''alucinación consensuada''*, un espacio no físico en el cual millones de personas interactúan a través de redes informáticas. A partir de esta primera aproximación surge la idea germinal de un entorno digital compartido que trasciende las distancias geográficas en tiempo real y de forma masiva. En 2001, la Real Academia Española en su 22° edición incluyó el término, definiéndolo como *''Ámbito virtual creado por medios informáticos''*.

Diversos autores especialistas en el área agregaron aspectos a estas concepciones a medida que abordaban el estudio de los diferentes matices del ciberespacio, como ser la dinámica de vínculos que se establecen en el ciberespacio. Manuel Castells, en *La Era de la Informática: Economía, sociedad y cultura* (1996), destaca el ciberespacio como la lógica espacial de la *sociedad-red*, enfatizando su dimensión de intercambio y redefinición de control social. Desde un enfoque más cultural, Pierre Levy en *Cibercultura* (1997), sostiene que *''El ciberespacio es un medio de comunicación interactivo que no se limita a un sustrato físico… …que amplía las capacidades cognitivas, imaginativas y comunicativas de la humanidad''.* De este modo, Levy destaca su potencial transformador, al posibilitar dinámicas relacionales y culturales propias del medio digital, superando las limitaciones geográficas, jurídicas y físicas.

El concepto, originado en la ciencia ficción, se ha normalizado progresivamente en el lenguaje popular a medida que más aspectos de la vida cotidiana -como la comunicación, el comercio o la gestión de recursos- se han digitalizado. Las definiciones hasta ahora expuestas coinciden en que el ciberespacio es:

- Un espacio de circulación e intercambio de datos informáticos permanente.

- Virtual e tangible.
- Supra geográfico y supra jurídico.
- Un entorno social, cultural y político.
- Un espacio donde emergen nuevas relaciones entre individuos, empresas, y gobiernos.
- Un entorno donde el ejercicio del control se ejerce de manera distinta al mundo físico.

A estas perspectivas se suma la visión de la OTAN, que enfatiza un punto de vista donde la ciberseguridad y las políticas de defensa tienen un rol más relevante: *‘’El ciberespacio es un dominio global dentro del entorno de la información compuesto por la interdependencia de infraestructuras de tecnologías de información, que incluyen internet, redes de telecomunicaciones, sistemas informáticos y dispositivos de control y comunicaciones’’.*

Esta última definición resalta la dependencia del ciberespacio de una infraestructura física sin la cual no podría existir tal como lo conocemos. Esta relación entre lo virtual y lo tangible da pie a la idea de una **Geopolítica del Ciberespacio**, con dos dimensiones principales: una geográfica (relativa a la ubicación de las infraestructuras) y otra política (relativa a su regulación y control).

En el **aspecto geográfico**, esas infraestructuras físicas están distribuidas globalmente con diferentes criterios, ya sean climáticos (de acuerdo a las necesidades de temperatura y humedad que precisan los servidores y centros de datos, por ejemplo) y de accesibilidad (los cables submarinos se conectan a tierra mediante estaciones de recepción ubicadas en las costas). Antenas, cables submarinos, servidores y centros de datos (algunos de ellos submarinos), centros de recepción costeros y demás infraestructuras tienen dueños (ya sea estatales o privados) y están sujetos a la soberanía de los países en los cuales se encuentran. , lo que implica que el dominio y control de la infraestructura también se extiende a ciertas dimensiones del ciberespacio.Y se trata de una tendencia ascendente: cada vez son más las tecnologías domésticas con acceso al Internet de las Cosas, al mismo tiempo que más y más países digitalizan gran parte de su burocracia y gestión de infraestructuras críticas. Sin mencionar que el creciente

desarrollo y aplicación de la Inteligencia Artificial demandará una más grande y compleja infraestructura física de ciberespacio.

En este contexto, es llamativo el hecho de que gran parte de esta infraestructura es privada. Un ejemplo son los cables submarinos, por donde circulan un 95 % de los datos de internet y telefonía actuales [1]. La introducción de la fibra óptica en reemplazo de los cables submarinos de cobre comenzó en 1988 con el TAT-8 (uniendo Estados Unidos con Francia y el Reino Unido), construido por un consorcio de varias empresas de telecomunicaciones entre las que destacó AT&T. La introducción de esta nueva tecnología correspondió al aumento de la cantidad y calidad de los datos transmitidos, coincidiendo con la masificación de líneas de teléfono domésticas (más tarde, incluso fue el primer cable en transmitir los primeros datos de internet privado, principalmente correos electrónicos). Desde esos comienzos hasta hoy, sólo un 20 % de los cables submarinos del mundo son de propiedad estatal, con un 59 % en manos privadas y el resto entre pequeños consorcios y otras entidades. Y así es que los cables submarinos representan la mejor tendencia en capacidad y calidad: la creciente conectividad cotidiana, y la mayor demanda de datos y rapidez de procesamiento (facilitados por las inteligencias artificiales) implicará un mayor ancho de banda y una menor latencia (retardo), compitiendo así con mucha ventaja contra otros sistemas de tráfico de datos (como satélites). Vamos hacia un mundo con más cables submarinos más eficientes y acaso también, nuestra dependencia de ellos (de las posibilidades que nos brindan) los transforma en un objetivo militar atractivo.

Otro caso interesante son los centros de recepción costeros o *landing stations*: se trata de estaciones en tierra que reciben los cables submarinos, adaptando el flujo de datos a la fibra óptica continental. Los países que poseen estas estaciones conservan una importante ventaja estratégica sobre aquellos países sin salida al mar que depende de estas estaciones para su acceso a internet. Por ejemplo, países como Afganistán, Armenia, Moldavia, Nepal, Bután y Kosovo dependen o bien de sus vecinos o de satélites para su acceso a internet. Otros son vulnerables ya que poseen una única vía (fibra óptica terrestre, en este caso) para su conectividad, tal es el caso de Yemen y Somalia. Un ataque directo contra esa única infraestructura de comunicación, y estos países quedarían aislados digitalmente. Es llamativo el hecho de que algunas naciones

[1] Mapa mundial de cables submairnos: https://www.submarinecablemap.com/

mencionadas sí cuentan con acceso al mar, pero sin poseer *landing stations.* Otros países mediterráneos, por ejemplo Chequia (República Checa) y Suiza, si bien no poseen salida al mar, están conectadas por varios cables terrestres a distintos países, lo que les asegura una diversificación de conexiones y redundancia en caso de conflicto armado, falla o sabotaje [2].

En el **aspecto político**, la Geopolítica del Ciberespacio aborda el estudio de las leyes y regulaciones que los estados u organizaciones internacionales aplican sobre el ciberespacio. La Gobernanza de Datos, así como la Diplomacia Cibernética, la Ciberseguridad, la Ciberinteligencia y la Soberanía Digital son manifestaciones del control y regulación que estados, empresas multinacionales y organizaciones internacionales pueden ejercer sobre la producción, circulación, almacenamiento y empleo de la información digital.

El poder fundamental de los estados nacionales y organizaciones internacionales, en relación a la Geopolítica del Ciberespacio, radica en su facultad de legislar. En cuanto a la gobernanza de datos, varios son los gobiernos y entidades internacionales que crearon marcos regulatorios, como por ejemplo la GDPR (*General Data Protection Regulation*) europea que busca proteger los privacidad de los usuarios en Internet, regulando el tráfico y uso de datos privados de las empresas de comunicaciones y redes sociales, o el *CLOUD Act* [3] (2018) de Estados Unidos, que regula el acceso a datos almacenados en servidores de empresas tecnológicas incluso si esos servidores están localizados fuera del país. Este último es un buen ejemplo de la dimensión transnacional tanto de los datos como de los alcances legales. En cuanto a la Soberanía Digital o Cibernética, ésta se define como el derecho de un estado a ejercer control y autoridad sobre las actividades, infraestructura y datos dentro de su territorio digital. La República Popular China ejerce soberanía cibernética a través de su Gran Cortafuegos, que regula y filtra el acceso a internet dentro de sus fronteras. Otro ejemplo es la Runet de Rusia, un proyecto en período de pruebas que busca controlar la conectividad interna del país y reducir la dependencia de proveedores externos: en 2024, se llevaron a cabo pruebas exitosas en la zona caucásica (Daguestán, Ingushetia y Chechenia) desconectando

[2] Nota: https://www.mapfreglobalrisks.com/en/risks-insurance-management/article/submarine-cables-the-true-communication-highway/
[3] Clarifying Lawful Overseas Use of Data.

temporalmente esta zona del internet global. En ese ensayo, servicios de mensajería y ciertos sitios de internet quedaron inaccesibles para la población.

Finalmente en el enfoque político, por Diplomacia Cibernética nos referimos al marco de cooperación internacional en el cual se proyectan, coordinan y definen estrategias internacionales que los estados utilizan para gestionar sus intereses en el ciberespacio. Entre estas estrategias, se discuten enfoques de ciberseguridad y ciberinteligencia conjuntas, gobernanza de datos, legislación sobre monopolios informáticos y mecanismos de respuesta internacional frente a amenazas y actores transnacionales.

El ciberespacio entonces, es una dimensión que puede ser afectada no sólo en la dimensión digital e intangible, sino también, por el control que se ejerce sobre sus infraestructuras físicas. Sabotaje de cables submarinos, hackeo (o destrucción) de satélites de comunicaciones, destrucción de antenas, así como leyes de almacenamiento de datos, marcos anti-monopolio, restricción de acceso a ciertos sitios de internet o bien, provisión de una intranet que se mantenga independiente de los servicios externos son ejemplos de cómo, tanto en la dimensión física como legislativa, el ciberespacio es un territorio donde también países, organizaciones y usuarios dirimen sus intereses.

Dicho lo anterior, al día de hoy existen varios ejemplos que ponen de manifiesto no sólo la relevancia, sino también la creciente tendencia del ciberespacio como un escenario donde ejercer presión. A continuación destacaremos aquellos episodios en los cuales el aspecto manipulado fue principalmente el físico. No porque sea más relevante, sino porque entre la literatura consultada para este artículo, es el aspecto menos abordado al menos desde una perspectiva geopolítica del ciberespacio.

En noviembre del 2024, el buque chino Yi-Peng 3, se vio envuelto en un escándalo internacional al coincidir su recorrido por el Mar Báltico con el mismo lugar de rotura de dos cables submarinos de fibra óptica[4]. Ambos cables fueron dañados en el plazo de 24 hs, ventana temporal dentro de la cual el mencionado transporte chino pasaba por el área. El gobierno chino de inmediato se prestó a la cooperación para la investigación, liderada por autoridades suecas, las cuales no emitieron una acusación directa al encontrarse el caso en investigación. Los efectos consistieron en el corte temporal de

[4] Precisamente, el C-Lion 1 (Alemania-Finlandia) y el BCS East-West Interlink (Lituania-Isla de Gottland, Suecia)

servicios de telefonía en Suecia y Lituania, proporcionando en este último, un tercio de la capacidad de internet del país. Ambos cables se restauraron a fines del mismo mes del corte. Dado que el barco chino implicado había estado reposando anteriormente en San Petersburgo, Rusia, las sospechas de un ‘’ensayo de sabotaje’’ caracterizaron el enfoque del problema.

Y no es el único caso que envuelve a Rusia. En un marco de lectura caracterizado por el actual conflicto de Ucrania y la creciente perspectiva de una amenaza a Europa por parte de Moscú, en junio de 2023 el ex presidente y actual vicepresidente del Consejo de Seguridad de Rusia, Dmitri Medvedev, declaró que no hay ninguna razón por la cual Moscú no debería destruir los cables submarinos del enemigo[5]. Esta declaración se basa en la supuesta complicidad de países occidentales en la destrucción de un segmento del gasoducto submarino Nord Stream[6], en setiembre de 2022, lo que demuestra que aunque en el mencionado caso hablamos de un gasoducto, sí deja en evidencia la vulnerabilidad de las infraestructuras submarinas (en nuestro caso, cables de fibra óptica). Además, en mayo del mismo año, la OTAN informó de la presencia de buques y submarinos rusos en zonas con densas concentraciones de cables en el norte de Europa y América del Norte, lo que sugiere posibles acciones de mapeo de infraestructura de comunicaciones por parte de Moscú[7].

En este contexto, la geografía rusa otorga una clara ventaja. Dado su continentalismo, Rusia basa su infraestructura de información mayoritariamente en medios terrestres. Países como Reino Unido, Taiwán, los países bálticos, Japón y Corea del Sur (entre otros aliados continentales), son especialmente vulnerables a ataques en sus cables submarinos, aunque disponen de sistemas redundantes. Dicho esto, en un probable futuro donde la infraestructura física del ciberespacio se transforme en un blanco militar recurrente, Rusia estaría menos expuesta, algo de lo que incluso el mismo Estados Unidos y varios aliados occidentales no podrían jactarse.

[5] Nota: https://www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14/

[6] El Nord Stream consiste en cuatro gasoductos divididos en dos trayectos, Nord Stream 1 y Nord Stream 2. Al momento de las explosiones, ninguno de los gasoductos estaba en operación, sin embargo, aún contenían cantidades marginales de gas que se elevaron a la superficie del mar.

[7] En octubre del mismo año, un cable que une Estonia con Suecia resultó dañado, en una región que coincidía con la anterior ubicación de varias naves rusas.

Reportes similares datan de abril de 2024, cuando de acuerdo al sitio Aviation24.com[8], aviones comerciales que volaban sobre el mar báltico experimentaron variaciones anómalas en sus sistemas de navegación de GPS (algunos incluso debieron aterrizar en emergencia), un problema que fuentes oficiales de Lituania conectaron con las capacidades de *jamming*[9] rusas en el vecino Kaliningrado, donde Moscú posee instalaciones fijas dedicadas a la guerra electrónica.

Los mencionados casos nos dan a entender que la amenaza a estas infraestructuras requiere de una cooperación entre las compañías privadas que las poseen y los gobiernos nacionales que puedan proporcionar la protección militar que las compañías privadas no pueden dar[10]. En este aspecto también es relevante el factor político, en forma de las regulaciones y controles que los estados ejercen sobre estas infraestructuras en función de su protección contra otros países o actores dañinos. Sin embargo, debemos recordar que gran parte de esos cables cruzan aguas internacionales, legalmente ajenas al control de los estados y de difícil vigilancia.

En Occidente, la compañía china Huawei se vio envuelta en el centro de discusiones geopolíticas dada la sospecha de que su prestación del servicio de 5G en países de Europa y en Estados Unidos (que consiste en la instalación y mantenimiento de antenas), podría tener propósitos ocultos de espionaje. En este contexto, Estados Unidos argumentó que la empresa china representa una amenaza para la seguridad nacional y prohibió la construcción de antenas en 2019. El Reino Unido prohibió a la empresa asiática en su red 5G exigiendo el retiro de su equipamiento para antes de 2027. Australia hizo lo propio, y Canadá tomó medidas similares en 2022. La relación entre esos países está dada por su cooperación de inteligencia, por lo que la vulnerabilidad de uno significa potencialmente un riesgo para el resto. Además, Washington sancionó a empresas proveedoras de semiconductores, prohibiendo la venta de chips avanzados a Huawei. Indirectamente, la producción y distribución de semiconductores, dada su

[8] Nota: https://www.aviation24.be/airlines/widespread-gps-interference-grips-european-airspace-suspicions-rise-over-russian-involvement/
[9] Término inglés para referirse a acciones de interferencia, negación o saturación de sistemas de transmisión como radares, radios, sistemas de posicionamiento global, etc.
[10] Nota: https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

relevancia en las infraestructuras físicas del ciberespacio, también constituye un interesante aspecto a analizar como parte de la Geopolítica del Ciberespacio[11].

Así como existen amenazas, también surgen medios para contrarrestarlas. Retomando el caso de los cables submarinos, en el norte de Europa están poniéndose a prueba sistemas digitales de vigilancia que permiten detectar con gran rapidez la ubicación de anomalías en el fondo del mar, lo cual podría significar acciones humanas directas sobre infraestructuras submarinas. Eso sumado a las medidas de redundancia temporal[12], como otros cables o redes privadas de satélites, como la red Starlink de Elon Musk, Kuiper de Amazon o OneWeb del Reino Unido[13].

El ciberespacio se nos revela como una dimensión en la cual pueden llevarse a cabo tantas tácticas y estrategias militares, psicológicas y de inteligencia como en el mundo físico. Si bien se trata de espacio intangible, ese espacio no puede existir sin la infraestructura física que lo soporta, y ésta está condicionada por la geografía y regulaciones. Dada la condición de que mayoritariamente estos medios físicos son de posesión privada, la cooperación entre compañías de telecomunicaciones y gobiernos que puedan proporcionar protección es vital. Sin embargo, como vimos antes, gran parte de esos medios se encuentran fuera del alcance legal de los países. La demanda y complejidad de estas infraestructuras seguirá creciendo al punto de que quizás, en el futuro, los ataques en estos medios tengan el mismo impacto que el uso de armas de destrucción masiva: aislamiento digital de países, ausencia o intervención en sistemas de navegación asistida, la posibilidad de sistemas de inteligencia masiva, de la militarización de centros de datos y servidores. Hablamos de instalaciones y medios inaccesibles para muchos estados, especialmente aquellas ubicadas en zonas internacionales, de difícil trazabilidad y dificultosa reparación.

Nuestra dependencia de estos medios no hará más que aumentar, y las infraestructuras físicas -y en menor medida, las políticas- del ciberespacio, pasarán a ocupar un rol protagónico en las disputas geopolíticas del siglo XXI.

---

[11] Nota: https://www.reuters.com/investigates/special-report/us-china-tech-cables/

[12] Los satélites no pueden manejar (por mucha diferencia) el mismo volumen de datos que los cables submarinos. Por esta razón, se los contempla como medidas temporales, priorizando las comunicaciones estratégicas y relativas a seguridad nacional en caso de la destrucción o negación de los cables submarinos tradicionales.

[13] Nota: https://www.businessinsider.com/elon-musk-starlink-satellite-internet-undersea-cables-not-extinct-tonga-2022-2