LABORATORIA
Revista de Ciencias Humanas

Humanidades
LICH-EH
UNSAM-CONICET

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

DOSSIER_GUERRA

El dilema de la definición. La necesidad de una polemología de la ciberguerra

The definition dilemma. The need for a polemology of cyberwar

Mgtr. Sol Gastaldi
Universidad de Buenos Aires
Buenos Aires, Argentina
sol_gastaldi@yahoo.com.ar

Recibido: 12/07/2024
Aceptado: 22/10/2024

Resumen

En un entorno de convergencia y dependencia cada vez mayor de las actividades del hombre de las tecnologías de la información y las comunicaciones, los Estados encuentran una serie de dilemas a la hora de planificar políticas y estrategias relacionadas con el uso del ciberespacio con fines militares, que consisten, básicamente, en la atribución de un ciberataque, la asimetría de capacidades, la colaboración público-privada para la ciberseguridad de infraestructuras críticas, la capacidad de ejercer la soberanía y la escasez de normas internacionales. No obstante, tras realizar un recorrido por dichos aspectos, y teniendo en cuenta que la definición guía la acción según las teorías de las políticas públicas, se plantea que el principal dilema radica en alcanzar una aproximación sobre qué es la ciberguerra.

Palabras clave: ciberespacio; ciberguerra; soberanía nacional; políticas públicas; tecnologías digitales.

Abstract

In an environment of convergence and increasing dependence of human activities on information and communications technologies, States encounter a series of dilemmas when planning policies and strategies related to the use of cyberspace for military purposes, which basically consist of the attribution of a cyber attack, the asymmetry of capabilities, public-private collaboration for the cybersecurity of critical infrastructures, the ability to exercise sovereignty and the scarcity of international standards. However, after reviewing these aspects, and taking into account that the definition guides action according to public policy theories, it is suggested that the main dilemma lies in reaching an approximation on what cyberwar is.

Keywords: cyberspace; cyberwar; national sovereignty; public policies; digital technologies.

LABORATORIA
Revista de Ciencias Humanas
Humanidades
LICH-EH
UNSAM-CONICET
Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Introducción

En 2010, el mundo asistió a un cambio del escenario de seguridad internacional: se conoció la primera arma cibernética empleada por un Estado contra otro Estado. Presuntamente, Israel y Estados Unidos utilizaron un programa informático, el "gusano" Stuxnet, para afectar el programa de enriquecimiento de uranio de Irán. A partir de ese momento, se inició una nueva carrera armamentista guiada por la adquisición y desarrollo de capacidades cibernéticas para ser empleadas de diferentes formas, de acuerdo a los objetivos políticos o militares. El mundo comprobó desde entonces operaciones de *ciberespionaje*, la disrupción de sitios web como sucedió en Estonia en 2007, daños a infraestructuras críticas tal como provocó Stuxnet, la manipulación de la opinión pública a través de las denominadas *fake news* y operaciones cibernéticas en conflictos armados, tal como en el caso de Rusia y Georgia en 2008 y, posteriormente, en la guerra entre Ucrania y Rusia iniciada en febrero de 2022.

Durante muchos años tomó protagonismo en los medios de comunicación y en gran medida también en la literatura especializada sobre el tema, la idea de que el mundo se encontraba atravesando una "ciberguerra fría" e incluso penetró en el imaginario el interrogante en torno a si era posible una guerra completamente "virtual".

Algunos analistas destacaron que, a pesar de los avances en drones de uso militar y sistemas de armas autónomas impulsados por el desarrollo de la inteligencia artificial, la guerra entre Rusia y Ucrania demostró que el actor con mayores cibercapacidades no renunció al empleo de armamento convencional para alcanzar sus objetivos operacionales (Valeriano, 2022). Como indica Boot (2006), los avances tecnológicos no podrán prescindir de "las botas en el terreno", así como tampoco podrá una computadora ocupar Montecassino (Albarracín Keticoglu y Eissa, 2019).

En su obra *Cyber war vs cyber realities* (2016), Valeriano y Maness relevaron los ciberataques ejecutados por Estados contra otros Estados. Los autores, que estudiaron conflictos entre Estados que llevaron en algún momento al empleo de ciberarmas, destacan que en ningún caso de los identificados ese tipo de conflicto derivó en una confrontación con medios convencionales. Otro autor, Thomas Rid (2012), estudió tres casos de ciberataques entre Estados de gran repercusión internacional y concluyó que ninguno de ellos puede ser considerado un ejemplo de *ciberguerra*. Rid toma el concepto de guerra de Karl von Clausewitz[1] y concluye que en ninguno de ellos se dieron los tres elementos identificados por el militar prusiano: motivación política claramente definida; empleo de medios violentos, y muertes y destrucción física.

Bajo este razonamiento, Rid considera que todos los ciberataques conocidos hasta la fecha pueden clasificarse como actos de sabotaje, espionaje o subversión, pero no como actos de guerra. Dicho esto, el autor afirma que el empleo de medios cibernéticos resulta una herramienta útil para tales operaciones –que se asemejan a las operaciones especiales de inteligencia y contrainteligencia–, por lo que le parece poco probable el desarrollo de una ciberguerra en el futuro.

1. Karl Von Clausewitz (2021) define a la guerra como un acto de violencia dirigido a obligar al oponente a cumplir nuestra voluntad. La violencia es una característica central para el autor, pues la considera como un duelo a gran escala. El otro elemento es el objetivo político: el que da origen a la guerra y establece la meta de la fuerza militar y el grado de esfuerzos a realizar, destacando así a la guerra como un acto político. Bajo este razonamiento, Clausewitz sostiene la consideración de la guerra como la mera continuación de la política por otros medios.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Si la probabilidad de desarrollo de una ciberguerra es escasa, ¿por qué entonces los países vienen adecuando sus políticas públicas, formulando políticas nacionales de ciberdefensa y estrategias de ciberseguridad, creando centros nacionales de respuesta a incidentes teleinformáticos e incluso unidades militares especializadas en ciberoperaciones o cibercomandos?, resulta que, los formuladores de políticas parten de la visión predominante de que el ciberespacio constituye un nuevo dominio que se entrelaza con los ambientes físicos tradicionales y que permite efectos operacionales, en el ciberespacio o bien fuera de él a la hora de diseñar e implementar estrategias, planes y programas para la defensa cibernética e incluso el desarrollo de capacidades ciberofensivas.

En un estudio previo, Gastaldi y Gioffreda (2020) analizaron los dilemas para los Estados-nación del uso estratégico del ciberespacio, identificando cuatro centrales: la posibilidad de identificar al atacante, la asimetría de capacidades, la colaboración público-privada y la escasez de regulación internacional. También se cuenta con los aportes de Gastaldi y Ocón (2019) y Gastaldi (2022) sobre la problemática del ejercicio de la soberanía nacional frente al fenómeno ciberespacial. El presente trabajo retoma los elementos allí analizados, para considerar un nuevo problema –y tal vez el más importante–: el de la definición misma de ciberguerra.

De esta manera, el presente artículo indagará, desde el prisma de la teoría de la hechura de políticas, la importancia de la definición de los fenómenos objetos de las políticas públicas. Particularmente, se reflexionará en torno de la importancia de definir la ciberguerra, lo cual constituye un problema político en sí mismo. A partir de un abordaje cualitativo, basado en el análisis documental y la revisión bibliográfica especializada como estrategia metodológica, se presentará esta cuestión bajo la consideración del problema como un dilema, pues en términos de formulación de políticas exigirá a los Estados la toma de decisión bajo incertidumbre respecto a un problema multifacético.

Entender los procesos de elaboración y evaluación de políticas públicas es relevante para comprender por qué algunos problemas reciben la atención de la sociedad y del Estado, cómo ingresan éstos en la agenda de gobierno, cómo son trabajados y cuáles son las respuestas que se elaboran para resolverlos. Siguiendo el enfoque de la teoría de hechura de políticas públicas, Sabatier (2007, p.3) señala que en el proceso "los problemas son conceptualizados y llevados al gobierno por soluciones; las instituciones gubernamentales formulan alternativas y seleccionan soluciones de políticas públicas; y aquellas soluciones implementadas, son evaluadas y revisadas". Esta afirmación revela la importancia de la conceptualización: al respecto, Aguilar Villanueva (1993) sostiene que la primera etapa del proceso es el reconocimiento del problema y su formulación como una construcción lógica que es estructurada de manera tal que tenga una respuesta o solución. Es decir, "la solución forma parte de la misma definición del problema" (Aguilar Villanueva, 1993, p.60):

> (...) la manera como se ha definido un asunto público condiciona la configuración de los instrumentos, modos y objetivos de la decisión

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

> pública, las opciones de acción. No es lo mismo definir, la pobreza como explotación, que como ausencia de igualdad de oportunidades o rezago cultural... Sus componentes y factores causales son diversos y perfilan políticas diversas (Aguilar Villanueva, 1993, p.52).

Es decir, cuando un problema ingresa en la agenda gubernamental, éste debe ser definido, entendiendo la definición del problema como el proceso por el cual una cuestión es estudiada, explorada, organizada y posiblemente cuantificada por los interesados (Aguilar Villanueva, 1993), por lo que

> (...) el problema de la definición de los problemas públicos es entonces doble. Por un lado, enfrenta la dificultad de construir y estructurar una definición aceptable, que supere los escollos de la polémica y pueda alcanzar de alguna manera consenso; por el otro, debe conducir a una definición operativa que dé pie y espacio a una intervención pública viable con los instrumentos y recursos a disposición del gobierno (Aguilar Villanueva,1993, p.57).

Teniendo en cuenta el aporte teórico mencionado, podemos afirmar que la definición de ciberguerra no será neutral, ni inocente. En su definición se encontrarán los actores, los medios y capacidades, alcances, normas y reglas que establecerán el empleo de operaciones cibernéticas con fines estratégico-militares.

Habiendo realizado esta introducción, el presente artículo se inicia con un apartado teórico en el que se indagará sobre qué espacio es el ciberespacio, a partir del establecimiento de sus características definitorias. Seguidamente, se exponen los dilemas que enfrentan los Estados en el empleo del ciberespacio con fines estratégicos, entre ellos, el objeto de este artículo: el dilema de la definición. Por último, se presentarán unas conclusiones dirigidas a la construcción de una polemología de la ciberguerra indagando nuevas dimensiones para la investigación, reflexión y el debate académico.

¿Qué espacio es el ciberespacio?

Gran parte de las definiciones de "ciberespacio" existentes, empleadas por gobiernos para la conceptualización de sus políticas de ciberseguridad y ciberdefensa, prescinden de los elementos político-estratégicos asociados a la propia naturaleza del ciberespacio (Gastaldi et al, 2018; Gastaldi, 2020b). Como ejemplo, el Departamento de Defensa de los Estados Unidos, define al ciberespacio como un dominio global compuesto por una red interdependiente de infraestructuras de información, que incluye internet, las redes de telecomunicaciones, procesadores y sistemas informáticos; y la Comisión Europea lo entiende como un espacio virtual por donde circulan los datos electrónicos de todos los ordenadores del mundo (Bejarano, 2011). Estas definiciones, que centran sus elementos en los datos, las redes, la información y procesadores, las

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

denominaremos definiciones de tipo *técnicas*, pues recurren a los aspectos tecnológicos del ciberespacio a partir de los cuales realizan su conceptualización.

No existe una definición consensuada del concepto de ciberespacio[2]. Esta situación es observada en la *Guía de Ciberdefensa* de la Junta Interamericana de Defensa –en adelante JID–:

> Muchos términos relacionados con el dominio "ciber" y el propio término y concepto "ciber" son actualmente controvertidos. No existe un único glosario de definiciones ni una taxonomía globalmente aceptada y como consecuencia, la mayoría de estudios relacionados con el ciberespacio y sus aplicaciones se ven en la obligación de incluir sus propios listados de definiciones. (JID, 2020, p.11)

El documento concluye que la "falta de consenso global de todo lo relacionado con el dominio ciber trae como consecuencia importantes disfunciones" (JID, 2020, p.11) Estas disfuncionalidades consisten en la existencia de visiones y perspectivas encontradas sobre lo que son las operaciones militares en el ciberespacio. Esto trae como correlato la dificultad de compatibilizar doctrinas, aspecto de gran relevancia al momento de pensar la interoperabilidad entre países, y complejiza la organización de las estructuras nacionales de ciberdefensa, lo cual impacta negativamente en la cooperación internacional.

> La información confusa y, a veces contradictoria, existente acerca de todo lo relacionado con el dominio 'ciber' dificulta la labor de las autoridades y directivos en el proceso de toma de decisiones (...) produciéndose, en muchos casos, resoluciones no idóneas o no adaptadas a la necesidad real. (JID, 2020, p.11)

Debido a la mencionada falta de consenso teórico, la *Guía de Ciberdefensa* (JID, 2020, p.17) acota la definición de ciberespacio a la de "entorno conceptual en el que se produce la comunicación a través de redes informáticas". Sin embargo, la JID precisa que "el ciberespacio es un concepto, idea o noción; no es un espacio material, físico, visible ni tangible". Y entonces su *materialización* se produce a partir de la interrelación de sus elementos específicos: infraestructura de tecnologías de información y comunicaciones, software, información, protocolos de transporte, energía eléctrica y las personas.

La definición anterior lleva a ponderar la idea de ciberespacio como fenómeno puramente cognitivo, que permite a los individuos tomar contacto con el ciberespacio y a partir de ese contacto se reconoce su existencia. Sheldon (2016, p.284) sostiene que muchas definiciones representan "el ciberespacio como un lugar informativo y virtual que existe dentro de una infraestructura que está implícita. Tales definiciones enfatizan el elemento cognitivo donde el ser humano interactúa directamente con la información creada, almacenada y transmitida dentro del ciberespacio" (la traducción

2. En un trabajo, Kuehl (2009) identifica catorce diferentes definiciones de ciberespacio.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

es propia), perdiéndose así la combinación de elementos físicos y cognitivos que caracteriza al ciberespacio.

De manera similar, algunos autores afirman que el fenómeno del ciberespacio no puede ser puramente cognitivo, ya que su materialidad parte de estructuras netamente físicas, como las computadoras, cables submarinos y fibra óptica. Tal como señala Ocón (2020), "el ciberespacio es un espacio cognitivo anclado en una esfera física y una lógica, donde tienen lugar las representaciones y las dinámicas de estas espacialidades, donde se estructuran las problemáticas, los dilemas y, en definitiva, el ejercicio del poder" (p.40).

La artificialidad del ciberespacio responde a una necesidad humana, y el uso que el hombre hace de esa artificialidad es su razón de ser. El ciberespacio es, entonces, un ámbito creado por el hombre para su uso pero que trasciende su existencia cognitiva, a consecuencia de su naturaleza dual.

Dualidad

Joseph Nye (2010, p.3) recoge esta materialidad dual en su definición de ciberespacio: señala al ciberespacio como un régimen híbrido único de propiedades físicas y virtuales, hecho por el hombre, que se caracteriza por poseer una infraestructura física –en la que rigen las reglas de la soberanía de los Estados– que da sustento a la infraestructura informacional, o virtual, a la que otros llaman también infraestructura lógica. De ahí que podamos caracterizar al ciberespacio como un ámbito *dual*: es virtual –cognitivo– y físico a la vez, en el que ambas esferas se relacionan y no es posible prescindir una de la otra (Gastaldi, 2020; 2021): no es una cosa o la otra, es ambas a la vez.

Transversalidad

Además de ser dual, el ciberespacio es *transversal*: ciertas dinámicas que ocurren en la capa virtual o lógica, tienen efectos sobre el mundo físico, lo que algunos autores denominan efectos cinéticos. Este atributo hace del ciberespacio un ámbito estratégico que los actores pueden emplear para el logro de determinados objetivos. El ciberespacio es así un ámbito para la acción (Gastaldi, 2021).

Esta transversalidad es aprovechada por *groomers*, ciberterroristas u otros actores no- estatales; es fuente de vulnerabilidades y de preocupación por parte de los responsables de la ciberseguridad de infraestructuras críticas, por la probabilidad de afectación de servicios esenciales como el suministro de energía, agua potable, servicios financieros, de salud, entre otros.

Como señala Ocón;

> La transversalidad del ciberespacio denota una dimensión fundamental de la intervinculación de los dispositivos y la esfera

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

> digital, es decir entre lo físico y lo ciberespacial. Existen acciones que se realizan desde los dispositivos técnicos que configuran diversas dinámicas en el ciberespacio, pero también, de forma inversa, existen acciones que se pueden realizar por medio del ciberespacio que afectan a los dispositivos técnicos. (Ocón, 2020, p. 61)

Globalidad

La interconexión de tipo reticular que construye al ciberespacio es de escala planetaria. Las barreras físicas tradicionales, límites geográficos o fronteras no existen en el ciberespacio. El desarrollo de internet, las comunicaciones inalámbricas y las redes sociales han dado origen a una nueva forma de comunicación horizontal, global e instantánea (Castells, 2010). El punto de inicio y el punto final de una vulnerabilidad o ciberoperación también poseen alcance global. Un claro ejemplo de ello fue la propagación del gusano informático Stuxnet que afectó el programa nuclear iraní a otros países. Justamente, el riesgo de diseminación a otros subsistemas es uno de los aspectos que hacen que las ciberarmas sean de uso limitado[3] (Valeriano y Maness, 2016).

Difusión del poder

La difusión del poder, refiere a la multiplicidad de actores que pueden llevar a cabo acciones en el ciberespacio (Nye, 2010). A diferencia dominio del mar, donde se requieren buques, del dominio aéreo donde se requieren aeronaves, o el espacio exterior donde se requieren satélites, para ingresar y actuar en el ciberespacio solo se precisa de un ordenador y conocimientos técnicos variables, de acuerdo a lo que se busque realizar, ya se trate de una comunicación, una transacción o un ciberataque. Y no son solo los Estados los que tienen capacidades para llevar a cabo operaciones cibernéticas hostiles. Organizaciones e incluso individuos, como Julian Assange que a través de Wikileaks logró afectar la política exterior estadounidense y cercenar la legitimidad de su intervención en Irak y Afganistán revelando el uso desproporcionado de la fuerza, o Edward Snowden, que expuso ante la opinión pública los programas de ciberespionaje que empleaba este mismo país.

Lo expresado muestra que el ciberespacio debe ser entendido por las características que le otorgan su materialidad y dinámica. Abogar por una definición estrictamente técnica, eliminaría su alcance lógico-cognitivo. Sin embargo, una definición estrictamente cognitiva, dejaría de lado su materialidad técnica. El ciberespacio es un ámbito artificial, creado por el hombre, que se caracteriza por ser dual, transversal y global y donde el poder se disemina de manera diferente a otros ambientes operacionales. Trasciende lo puramente cognitivo, lo físico y lo virtual. Además, como todas las creaciones del hombre, tiene un fin. Es ese fin, precisamente, el que permite avanzar hacia una consideración operacional del ciberespacio, es decir, un ámbito para la acción y el logro de objetivos.

3. Valeriano y Maness (2016) consideran que los países que disponen de estas capacidades hacen un uso restringido del mismo debido, principalmente, a las propias características de las ciberarmas. Al respecto mencionan que una vez empleadas, el código queda expuesto y pueden ser desarrolladas y empleadas por otros actores; también resulta difícil limitar los daños, pues estos programas pueden afectar otras infraestructuras ajenas a las del blanco, con riesgo de disipación en el ámbito civil. Una última explicación al uso limitado está relacionada con un análisis de costo-beneficio al momento de hacer una operación cibernética de gran envergadura como fue Stuxnet, pues en muchos casos son operaciones costosas y que requieren mucho tiempo de planificación y ejecución, y en algunos casos exigen montar estructuras similares para probar la eficacia de los programas antes de su uso. Kravetz (2023) realiza un estudio detallado de la Operación Olimpic Games y la compara con la denominada Operación "Opera", un ataque preventivo que ejecutó Israel en junio de 1981 contra un reactor nuclear iraquí. En ambos casos el objetivo estratégico se cumplió –dañar al reactor–, aunque la operación Olimpic Games que empleó Stuxnet llevó 48 meses ejecutarla, mientras que la Operación Ópera sólo 18 meses.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Dilemas estratégicos

Retomando, el ciberespacio se caracteriza por la difusión del poder. Múltiples actores pueden emplear recursos informáticos interconectados electrónicamente para lograr efectos deseados en o desde el ciberespacio, lo que fue analizado por diversos autores como el elemento clave del ciberpoder (Khuel, 2009; Nye, 2010). Nos interesa aquí abordar los desafíos estratégicos que encuentran los Estados en la dinámica ciberespacial, a la hora de realizar operaciones cibernéticas o administrar los efectos de un ciberataque. Si bien no se trata de un recorrido exhaustivo por todas las dificultades o disyuntivas que éstos pueden encontrar, examinaremos a continuación aquellos que, a nuestro entender, son clave para el análisis de políticas públicas de defensa y toma de decisiones de tipo estratégicas. En este marco, y basándonos en estudios previos (Gastaldi y Gioffreda, 2020; Gastaldi y Ocón, 2019 y Gastaldi, 2022), abordaremos de manera resumida el dilema de la atribución, la cuestión de la asimetría, la cooperación público-privada, el vacío normativo internacional y las capacidades para administrar la soberanía nacional, para profundizar en el nuevo dilema que planteamos aquí: el dilema de la definición.

En primer lugar, hay tres interrogantes básicos que plantea un ciberataque para un Estado: conocer el quién, el dónde y cómo responder, lo que se encuentra estrechamente ligado al dilema de la atribución, es decir la capacidad para identificar al responsable de un ciberataque.

Sin embargo, la mayor parte de los autores y especialistas coinciden en que si bien no es posible establecer con exactitud al atacante –si éste busca ocultar su identidad en el ciberespacio–, mediante el empleo de técnicas de informática forense complementado con el análisis de inteligencia es posible atribuir el ciberataque con cierta certeza. En este marco, el dilema que encuentran los Estados es, por un lado, que la falta de atribución puede dejar al Estado indefenso y expuesto a nuevas vulnerabilidades. Por otro lado, la atribución genera otro desafío: cómo responder al ciberataque. Asimismo, y dado que se trata de ciberataques de autoría oculta o encubiertas, el atacante puede rechazar la atribución o tratarse de un caso de *falsa bandera*.

En cuanto a la asimetría, sostuvimos que cualquier persona con un ordenador y conocimientos técnicos puede operar en el ciberespacio, lo que hace de este dominio un ámbito eminentemente asimétrico, con actores que no podrían ser confrontados en un escenario convencional. Si bien muchos especialistas consideran que sólo los Estados centrales poseen las capacidades tecnológicas, económicas y recursos necesarios para ejecutar ciberoperaciones de gran magnitud, como la que afectó el programa de enriquecimiento de uranio de Irán, lo cierto es que el mundo ha atestiguado ejemplos de infraestructuras críticas afectadas por grupos criminales, como fue el caso de Colonial Pipe en 2021 e incluso por individuos aislados. En este sentido, contrastan las opiniones entre aquellos que sostienen que en el ciberespacio se replican las asimetrías de poder convencionales, y los que ponderan los márgenes para la acción de la multiplicidad de actores que en ámbitos tradicionales no tendrían oportunidades.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

El siguiente dilema parte de la necesidad de los Estados de gestionar la ciberseguridad y la ciberdefensa de infraestructuras críticas –aquellas cuya interrupción podría afectar la estabilidad económica y el bienestar de una nación–, con los administradores de las mismas, generalmente en manos de privados. Un ejemplo común en estos casos es la falta de protocolos o incentivos –o altos costos en términos de confianza– para denunciar los ciberataques por parte de las empresas afectadas, así como también el tratamiento de información sensible o reservada.

En cuarto dilema se relaciona con la falta de normas internacionales sobre conducta estatal responsable en el ciberespacio. Si bien ha habido avances de importancia en la materia relacionados con la denominada *ciberpaz* y la *ciberdiplomacia*, así como en los ámbitos de la seguridad internacional y los Derechos Humanos (tales como las resoluciones de la Asamblea General de las Naciones Unidas referidas al Derecho a la Privacidad en la Era Digital, o sobre la Promoción, Protección y Disfrute de los Derechos Humanos en Internet, entre otras) aún no existe un esquema normativo que permita establecer con claridad qué acciones estatales en el ciberespacio son aceptables por la comunidad internacional y cuáles podrían ser consideradas hostiles y violatorias del derecho internacional.

En quinto lugar, se presenta el dilema vinculado con el ejercicio de la soberanía nacional en el ciberespacio. Si bien la soberanía de los Estados sobre la capa física del ciberespacio es indiscutible, esta se torna más difuso su ejercicio en la capa lógica o virtual. Esta es una esfera globalizada en la que impera la anomia e intervienen diversidad de actores, incluidos también los ciberactores o ciberpersonas que sólo existen materialmente en el ciberespacio y se expresan desde ciberidentidades. Más allá de la relación que se observa en este dilema con la visión de las capas del ciberespacio, existe otro desafío vinculado con la creciente convergencia digital, la cual consiste en la desaparición de barreras técnicas entre dispositivos electrónicos que transmiten información digital (Ibañez, 2006).

Con la expansión de las tecnologías digitales, incluida el internet de las cosas (IoT) y la inteligencia artificial, esta convergencia se encuentra trasladándose al mundo físico, creando un nuevo paradigma socio-cultural, en el que es cada vez es más difícil separar el mundo real del mundo virtual (Gastaldi, 2021). Bazzara (2021) analiza este emergente paradigma al que denomina como streamificación de la cultura, al que considera como resultante de la progresiva instalación de técnicas informáticas basadas en los datos y algoritmos durante la primera década de nuestro siglo y los múltiples y diarios usos sociales que éstos permitieron posteriormente.

Como señalamos en Gastaldi y Ocón (2019), la tendencia hacia un mundo en el que convergen en tiempo real una multiplicidad de ámbitos y actividades, personas y cosas, en plataformas digitales es irreversible.

Este nuevo paradigma surge de "la constante expansión de la esfera digital sobre las múltiples dimensiones de la vida humana y la dependencia cada vez mayor de las sociedades de tales plataformas tecnológicas" (Gastaldi, 2020b, p. 99).

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Así las cosas, afirmamos que:

> La globalización, inicialmente asociada a los procesos económicos mundiales, principalmente financieros, se ha expandido a través de internet hacia la esfera societaria dando lugar al desarrollo de verdaderas comunidades globales a través de redes sociales, que escapan a la acción de cualquier Estado-nación, comunidades globales que trascienden nacionalidades, fronteras, y la autoridad y la soberanía territorial de los Estados en tanto se encuentran alojadas en el denominado ciberespacio (Gastaldi, 2020b.) Sin ánimo de afirmar que el paradigma de la convergencia ha desplazado al paradigma de la globalización, sino que podría consistir en la fase tecnológica de la globalización, sobre la base de un novedoso ensamblaje entre la materia física, los hombres y los datos. Tal como la globalización en sus inicios representó una trasformación radical en la articulación entre soberanía y territorio, a partir de la descentralización de la soberanía y la desnacionalización parcial del territorio (Sassen, 1996), hoy la convergencia también supone una nueva trasformación en la articulación entre soberanía y territorio.

En este punto, Gendler (2016) señala que el concepto de "globalización" como objeto de estudio académico e incluso a nivel coloquial ha perdido relevancia frente al auge de nuevas teorías y enfoques, como el de la Sociedad de la Información, el capitalismo informacional, el capitalismo cognitivo, la sociedad red, entre otras, y ha quedado al margen de los estudios relacionados con las tecnologías digitales, pese a estar relacionadas con el fenómeno de la globalización.

En términos políticos, el paradigma de la convergencia podría suponer una transformación en la articulación entre soberanía y territorio sobre la base de la desterritorialización de la soberanía. En otras palabras, el nuevo paradigma conduce a una nueva forma de ejercer la soberanía a partir de la convergencia entre el espacio físico y el virtual. Así, "el hecho de que las prácticas de soberanía que desarrollan los Estados se hayan orientado históricamente hacia la producción de espacios territoriales diferenciados, afecta a la conceptualización de lo que estos deben proteger" (Gastaldi, 2020b, p. 109, en referencia a Wendt, 2005, p.23).

El dilema de la definición

En sexto lugar, encontramos el dilema de la definición. "El asunto de definir el ciberespacio no es trivial. Lo que decidimos incluir o excluir del ciberespacio tiene implicancias significativas, dado que determina el alcance de las estrategias del ciberespacio y las operaciones de ciberpoder", afirma Sheldon (2016, p. 285. La traducción es propia). Es decir que la dificultad de entender el ciberespacio se traslada inevitablemente al campo de las políticas públicas, a la posibilidad de

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

diseñar e implementar políticas que logren establecer los mecanismos adecuados para el bien a proteger.

Comprender erróneamente la materialidad del ciberespacio, las posibilidades y límites del ejercicio de la soberanía, las capacidades que brinda para la acción estratégica, incluso las características de los actores y sus objetivos, puede conducir a políticas erráticas o inadecuadas en materia de ciberseguridad y ciberdefensa, así como también a la hora de planificar el empleo de la fuerza en una guerra cibernética. En este mismo sentido, Reale (2023, p. 91) afirma: "La ciberguerra también tiene desafíos propios que se traducen en dificultades al momento de abordarla. Su opacidad genera incertidumbre en el diseño y planeamiento de acciones por parte de los tomadores de decisión".

Reale (2023, p.73) explica de manera clara la visión predominante de los Estados al respecto: "los Estados consideran al ciberespacio como un dominio que debe ser defendido frente a operaciones militares cibernéticas de otros países que puedan ser consideradas actos de ciberguerra, así como para prevenir tales actos de manera proactiva mediante la generación de mecanismos que aumenten la capacidad ciberdefensiva". Pero, ¿qué es un acto de ciberguerra?, pregunta que nos lleva nuevamente al dilema de la ausencia de normas internacionales vinculantes sobre la conducta estatal y el alcance del derecho internacional humanitario. Frente a la ausencia de consensos internacionales, el ciberespacio aparece como un estado de naturaleza, y los alcances de la ciberguerra se tornan difusos. Frente a su opacidad militar (Reale, 2023), la ciberguerra es tan heterogénea como el ciberespacio que le da lugar.

La definición entonces guía los modos de abordar la problemática y moldean la conducta del actor estatal en el ciberespacio. Es más, puede incluso contribuir a la construcción de percepciones en torno a los niveles de ciberconflicto. Así, definiciones más amplias o laxas de ciberguerra pueden conducir a percepciones en torno a la existencia de altos niveles de ciberconflicto, lo que conlleva a políticas dirigidas a militarizar el ciberespacio (Gastaldi y Eissa, 2020). Contrariamente, definiciones más restrictivas terminan por considerar a la ciberguerra como un fenómeno poco frecuente (Valeriano y Maness, 2016) e incluso, inexistente o de baja probabilidad de ocurrencia (Rid, 2012). Además, algunos autores consideran que la ciberguerra no necesariamente sucede en paralelo a la guerra convencional (Reale, 2023; Feliú Ortega, 2012), lo que generaría una inconcebible incertidumbre desde el plano del derecho internacional humanitario que regula justamente los conflictos bélicos interestatales.

Aguilar Villanueva señala:

> La tarea política de líderes, partidos y organizaciones es cómo hacer para que los que padecen inmediatamente la situación y otros grupos interesados pasen de la vivencia de la situación problemática al concepto del problema, a una definición para ellos plausible, convincente. Tarea no diversa a la que enfrentan gobernantes y

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

> analistas de políticas. También ellos tienen que ofrecer información, conocimientos, ejemplos, argumentos, que ayuden a los grupos sociales afectados a abandonar la simple indicación o denuncia de la situación problemática, molesta e irritante, y a entender y aceptar una definición del problema que permita intervenir sobre ella. Los gobiernos y sus analistas deben construir definiciones de problemas aceptables y solubles, legal y políticamente aceptables, fiscal y administrativamente viables (...) De todos modos, es un permanente dolor de cabeza de los políticos responder a la pregunta si el gobierno debe seguir la definición que posibilita el tratamiento efectivo del problema o la que políticamente le resulta menos costosa aunque no eficaz. La identidad entre eficacia y consenso seguirá siendo un concepto límite. (1993, p.59)

Siguiendo la definición anterior, podemos pensar que más allá de las múltiples definiciones de ciberguerra, los Estados construirán sus definiciones en función de su idiosincrasia, normas, intereses y recursos disponibles. El dilema está, justamente, en poder establecer una definición útil a los mismos. Tal vez, sea ese el motivo por el cual la Guía de Ciberdefensa de la Junta Interamericana de Defensa que mencionábamos al inicio, no aporta una definición. Una búsqueda por palabra clave en ese documento, arroja como resultado que el término ciberespacio aparece doscientos dieciséis veces, ciberamenaza cuarenta y cinco veces, ciberriesgo veintiséis, y ciberguerra, ninguna. En relación con el derecho internacional humanitario, el citado manual menciona las problemáticas asociadas a la aplicación del mismo y las diferentes posturas de los países que hacen difícil establecer consensos, pese a que en general, es aceptado que "una ciberoperación que cause graves daños a los intereses nacionales puede ser considerada un ataque armado, aún en ausencia de bajas humanas, y consecuentemente puede aplicarse el derecho a la legítima defensa y desencadenar una represalia militar legítima y proporcionada de cualquier ámbito, convencional o ciberespacial" (JID, 2020, p. 98), y que "las ciberoperaciones ofensivas siguen siendo en muchos países un asunto controvertido, a pesar de que es globalmente reconocido de que están sujetas a las mismas normas y principios del derecho internacional que las operaciones militares convencionales" (JID, 2020, p. 98).

Conclusión

En el ciclo de desarrollo de las políticas públicas, la definición del problema es tan crucial como su respuesta. Dicha definición encarna los procedimientos y recursos que el gobierno adoptará para dar cuenta de la problemática a través de la implementación de una política. En tal sentido, en este trabajo planteamos la definición de ciberguerra como un dilema: sin nociones claras de lo que ésta abarca, probablemente las políticas de ciberdefensa desarrolladas por los Estados no logren proteger adecuadamente al país en el ciberespacio.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

La falta de acuerdos internacionales en la materia aumenta aún más esta problemática, al igual que los otros dilemas que el Estado debe atender: los alcances de la soberanía, la cuestión de la asimetría, la cooperación con el sector privado en la ciberseguridad de las infraestructuras críticas y el establecimiento de la atribución. Todo ello genera un complejo escenario en el que el Estado debe orientar su *policy making* para garantizar tanto la defensa de su ciberespacio como el uso del ciberespacio para su defensa nacional.

Éstas últimas dos funciones –defensa del ciberespacio y uso del ciberespacio para la defensa nacional– involucran una serie de actividades relacionadas al menos con tres dimensiones: inteligencia, operaciones de información y operaciones militares convencionales. Algunas de éstas quedarán en manos de las agencias de inteligencia estratégica del nivel estratégico nacional; otras bajo responsabilidad de las Fuerzas Armadas, de acuerdo a las normativas de cada Estado.

En cuanto a la primera dimensión –inteligencia–, algunos países recurren al uso del ciberespacio –en tiempo de paz y guerra– para la producción de inteligencia, ya sea inteligencia de amenazas y/o ciberinteligencia, mientras que otros también para el desarrollo de operaciones especiales de inteligencia, tales como el sabotaje, espionaje o subversión (Kravetz, 2023).

En cuanto a las operaciones de información, cabe señalar que existe una tendencia militar global a separar estas operaciones de las de inteligencia. Dicho esto, podemos encontrar el uso del ciberespacio en apoyo a las operaciones de comunicación social o bien realizar acciones de propaganda, desinformación, influencia, decepción, intoxicación informativa u operaciones psicológicas. Nye (2018) hace referencia a la interferencia rusa en las elecciones de Estados Unidos en 2018 como ejemplo de uso del ciberpoder de manera malintencionada con el propósito de influir sobre una audiencia manipulando la información, o poder punzante.

La tercera dimensión corresponde a las operaciones militares convencionales, y es aquí donde aparece el uso de las operaciones cibernéticas de tipo ofensivas, para afectar las capacidades del enemigo. Éstas poseen un rol cada vez más importante, a medida que avanzan las concepciones doctrinarias y de empleo de las fuerzas armadas en las operaciones multidominio. El ciberespacio aparece como un dominio específico, pero con capacidades de afectar los otros ámbitos de operaciones, gracias a su dualidad y convergencia.

Con relación a esta última dimensión, encontramos un paralelismo entre ciberguerra y guerra electrónica. Si bien no puede desarrollarse una guerra exclusivamente electrónica, tampoco una guerra únicamente cibernética. En resumidas cuentas, la guerra electrónica refiere a las medidas y contramedidas de empleo del espectro electromagnético para afectar las comunicaciones y sistemas radar del enemigo –o para proteger los propios–; del mismo modo, la ciberguerra debería referir a aquellas acciones destinadas a afectar la disponibilidad, confiabilidad e integridad de los activos digitales –redes, sistemas e información– de los medios del enemigo, y las defensas de los propios, mediante programas informáticos.

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Por lo expuesto, la defensa del ciberespacio y uso del ciberespacio para la defensa nacional involucra acciones de ciberguerra, pero no debería ésta confundirse con el empleo del ciberespacio para tareas de inteligencia o para el desarrollo de operaciones de información. Ni tampoco con las necesarias acciones de ciberseguridad para proteger los sistemas e información propios, como cualquier organización. La consideración de la ciberguerra como un fenómeno que involucra estas actividades –inteligencia, operaciones de información y ciberseguridad– conlleva, en nuestro análisis, a un concepto que oscurece, en vez de esclarecer.

Es así entonces que concluimos en la necesidad de avanzar en el establecimiento de una polemología de la ciberguerra, para poder conocer de manera científica el fenómeno, pues el desorden terminológico existente termina vaciando de contenido al concepto, y englobando dentro del fenómeno de la ciberguerra a ciertos sucesos que nada tienen que ver con la guerra.

¿Es la ciberguerra la fase virtual de la guerra? Si un actor no estatal afecta la infraestructura de electricidad de un país, ¿es un caso de ciberguerra? Si una agencia de inteligencia realiza una infiltración sobre la red interna de otro país, ¿es un ejemplo de ciberguerra? Si un actor realiza una acción de denegación de servicio distribuido sobre la página web del ministerio de defensa de un país, ¿es un ejemplo de ciberguerra? Justamente, englobar fenómenos diversos bajo el mismo concepto trae confusión. En este orden de ideas, sería un grave peligro para los Estados que esta confusión o desorden terminológico se termine trasladando al campo de las políticas públicas.

Sartori (2008) mencionaba en un artículo el problema de la transferencia relacionado con la ampliación de los fenómenos a estudiar por la ciencia política. En cierta medida, es posible preguntarse si el concepto de ciberguerra no ha sido sacrificado por el estiramiento conceptual quedando éste vago y amorfo. Como señala el autor citado “mientras un concepto general conduce a la generalización científica, las meras generalidades, por el contrario, conducen solo a la vaguedad y confusión conceptual” (Sartori, 2008, p.38).

A pesar de que sigue estando pendiente el estudio sistemático del fenómeno de la guerra en el ciberespacio, los Estados continuarán avanzando en el diseño de políticas y acciones públicas concretas, sorteando con distinto grado de éxito el dilema de la definición, en función de sus objetivos estratégicos, marcos normativos, capacidades y recursos.

Bibliografía

Aguilar Villanueva, L. (1993). “Estudio introductorio”. En Aguilar Villanueva, Luis A. (comp.). *Problemas Políticos y Agenda de Gobierno* (pp. 15-71). Ed. Miguel A. Porrúa.

Albarracín Keticoglu, A. y Eissa, S. (2019). "Quo vadis Ciberdefensa. Apuntes estratégicos". *Revista de Estudios Políticos*, 114-131.

Bazzara, L. (2021). "Datificación y streamificación de la cultura. Nubes, redes y algoritmos en el uso de las plataformas digitales". *In Mediaciones de la Comunicación*, 16 (2), pp. 37-61.

Bejarano, M. J. (2010). "Alcance y ámbito de la seguridad nacional en el ciberespacio". *Cuadernos de Estrategia*, 149, pp. 47-82.

Boot, M. (2006). "The paradox of military technology". *The New Atlantis*, 14, pp. 13-31.

Castells, M. (2010). *The information age. Economy, society and culture*. Wiley-Blackwell.

Clausewitz, K. V (2021). *De la guerra.* Ediciones Obelisco.

Feliú Ortega, L. (2012). "La ciberseguridad y la ciberdefensa. El ciberespacio, nuevo escenario de confrontación". *Monografías del CESEDEN*, 126, pp. 37-69.

Gastaldi, S., et. al. (2018). "Ciberdefensa y soberanía nacional: indagando teorías y definiendo conceptos". *Primeras Jornadas de Ciencia y Tecnología de la Universidad de la Defensa Nacional*. Buenos Aires, 28 de julio.

Gastaldi, S. (2020a). "Introducción". En Gastaldi S., Ocón L (Coord.) (2020) *Ciberdefensa. Claves para pensar una estrategia de soberanía nacional* (pp. 29-36). TAEDA.

Gastaldi, S. (2020b). La soberanía en un mundo convergente. Apuntes para entender los dilemas para la seguridad y la defensa. En Bellomo, S., Oszlak, O. (Ed.) *Desafíos de la administración pública en el contexto de la Revolución 4.0* (pp. 85-118). Konrad Adenauer Stiftung.

Gastaldi, S. y Eissa, S. (2020). Relaciones internacionales y ciberespacio ¿Enfoques teóricos en pugna? En Gastaldi, S., Ocón, L. (Coord.) (2020). *Ciberdefensa. Claves para pensar una estrategia de soberanía nacional* (pp. 125-158). TAEDA.

Gastaldi, S y Gioffreda, C. (2020). La naturaleza estratégica del ciberespacio. Desafíos y dilemas para la toma de decisiones. En Gastaldi, S., Ocón, L. (Coord.) (2020). *Ciberdefensa. Claves para pensar una estrategia de soberanía nacional* (pp.97-124). TAEDA.

Gastaldi, S. y Ocón, L. (2019). "Ciberespacio y Defensa Nacional: una reflexión sobre el dilema libertad-seguridad en el ejercicio de la soberanía". En *Defensa Nacional. Revista científica*, 02, pp. 88-109.

Gastaldi, S. (2021). "La soberanía nacional frente al escenario de convergencia digital. Dilemas y desafíos para los Estados". En *Revista de la ESG*, 21, pp. 102-111.

Gendler, M. A. (2016). Globalización y tecnologías digitales: Un estado de situación. *Unidad Sociológica*, 6

Nº1 NOVIEMBRE 2024
E-ISSN: 3072-6727

Junta Interamericana de Defensa (2020). *Guía de ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. Junta Interamericana de Defensa.

Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem" en, Franklin Kramer, Stuart H. Starr y Larry Wentz (eds), *Cyber power and National Security*, National Defense University Press y Potomac Books. pp. 24-42

Kravetz, J. (2023). Operaciones especiales en el ciberespacio: espionaje, sabotaje y subversión en el siglo XXI. *Revista de la Escuela Nacional de Inteligencia*, 3, pp. 35-64.

Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Nye, J. (2010). *Cyber power*. Bedfer Center for Science and International Affairs. Harvard Kennedy School, May 2010.

Nye, J. (2018). How sharp power threatens soft power. *Foreing Affais*. https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power

Ocón, L. (2020). Abracadabra y la Biblioteca de Babel: aproximación geopolítica a la espacialidad del ciberespacio. En Sol Gastaldi y Leandro Ocón (Coord.) *Ciberdefensa. Claves para pensar una estrategia de soberanía nacional* (pp. 37-72). TAEDA.

Ocón, L., Verly, F. y Albarracín Keticoglu, A. (2020). Soberanía, autonomía y ciberespacio. ¿Nuevos desafíos? En Sol Gastaldi y Leandro Ocón (Coord.) *Ciberdefensa. Claves para pensar una estrategia de soberanía nacional* (pp. 213-232). TAEDA.

Reale, J. (2023). Los desafíos de la ciberguerra y la importancia de fortalecer la inteligencia estratégica militar en la Argentina. *Revista de la Escuela Nacional de Inteligencia*, 02, 66-100.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35 (1).

Sabatier, P. (2007). The need for better theories. En P. Sabatier (ed.) *Theories of the policy process* (pp. 3-17). Westview Press.

Sartori, G. (2008). Falta de formación conceptual en política comparada. *Revista Latinoamericana de Política Comparada*, 1, 17-65

Sassen, S. (1996). *Losing control? Sovereingty in an Age of Globalization*. Columbia University Press.

Sheldon, J. B. (2016). The rise of cyberpower. En J. Baylis; J. Wirtz; C. Gray (Eds). *Strategy in the contemporary world* (pp. 291-307). Oxford University Press.

Thornhill, J. (2020, 06 de abril). COVID-19 está acelerando el paso al 'teletransporte'. *Financial Times.*

Valeriano, B., Maness R. (2016). *Cyber war vs cyber realities. Cyber conflict in the international system*. Oxford University Press.