CIBERESPACIO Y DEFENSA NACIONAL: UNA REFLEXIÓN SOBRE EL DILEMA LIBERTAD-SEGURIDAD EN EL EJERCICIO DE LA SOBERANÍA[1]

ALFREDO LEANDRO OCÓN

Licenciado en Ciencia Política (Universidad de San Andrés) Mag. en Estrategia y Geopolítica. Profesor titular del Seminario Ciencia y Tecnología aplicada a la Defensa de la Maestría en Defensa Nacional de la Facultad de la Defensa (FADENA) de la UNDEF, profesor titular de la materia "Nuevos Escenarios de las Relaciones Internacionales" en el Colegio Militar de la Nación (CMN) y profesor e investigador en la Escuela Superior de Guerra de Ejército (ESG). Investigador acreditado UNDEF.

SOL GASTALDI

Licenciada en Ciencia Política (Universidad de Buenos Aires). Mag. en Defensa Nacional. Profesora titular del seminario "Ciencia y Tecnología aplicada a la Defensa" de la Maestría en Defensa Nacional de la Facultad de la Defensa (FADENA) de la UNDEF y profesora en la materia "Defensa y seguridad. Una mirada desde las relaciones internacionales y las Políticas Públicas" de la carrera de Ciencia Política de la UBA. Investigadora acreditada UNDEF.

Introducir en el planeta una nueva civilización y esperar luego paz y tranquilidad significa el colmo de la ingenuidad estratégica.
(Toffler, A. y H., 1994, p. 42)

Resumen

Este artículo tiene por propósito abordar el debate respecto del dilema li

1 Este artículo fue elaborado en el marco del proyecto "Soberanía Nacional y Ciberdefensa. Elementos teóricos y político-estratégicos del desafío ciberespacial para la Defensa Nacional", Programa de Acreditación y Financiamiento de Proyectos de Investigación "UNDEFI" de la Universidad de la Defensa Nacional (UNDEF). Amplía aspectos trabajados en el libro *Ciberespacio, Estrategia y Defensa Nacional,* de próxima publicación.

bertad-seguridad en el ciberespacio, desde la óptica de la Defensa Nacional. Para ello, se presenta la idea de convergencia digital y de los límites que esta encuentra por parte de los Estados a raíz de los riesgos y amenazas que se presentan en o desde el ciberespacio. En consecuencia, se indaga sobre los alcances de la soberanía en la época actual y las posibilidades de alcanzar márgenes de autonomía en el ciberespacio para países periféricos, ofreciéndose al final una reflexión sobre el ejercicio del poder y la soberanía estatal en torno a una nueva agenda de investigación para la Defensa.

Palabras clave:

Defensa Nacional - soberanía - ciberespacio - convergencia digital - autonomía.

Abstract

This paper aims at addressing the debate on the freedom-security dilemma in cyberspace, from the perspective of National Defense. To that end, the idea of digital convergence is introduced, and its limits imposed by the States as a result of the risks and threats that occur in or from cyberspace. Consequently, it explores the scope of sovereignty in the current era and the possibilities of reaching margins of autonomy in cyberspace for periphery countries, offering a final reflection on the exercise of power and state sovereignty regarding a new research agenda for defense.

Keywords

National Defense - sovereignty - cyberspace - digital convergence - autonomy.

Introducción

La Defensa Nacional es una actividad indelegable de los Estados que tiene, entre otros fines, el de preservar la soberanía. La época actual, marcada por el predominio de las tecnologías de la información y de las comunicaciones en todos los ámbitos de la vida humana, ha generado un desafío no solo a esta categoría en términos teóricos sino también prácticos, puesto que la

mayoría de los países se han encontrado obligados a introducir nuevas políticas para garantizar la defensa nacional frente a los riesgos y amenazas que se plantean en el ciberespacio.

En el plano virtual, las fronteras de los Estados son atravesadas por flujos de información; en el plano físico, por infraestructuras tales como los cables submarinos y las redes de fibra óptica que dan soporte a internet, la principal tecnología de la información de nuestra era. Nuevos centros y periferias aparecen en el marco de la convergencia digital del siglo XXI, entendiendo por esta la multiplicidad de los ámbitos atravesados y sostenidos por plataformas de información que convergen en tiempo real y sin fronteras en el ciberespacio, como el comercio y finanzas internacionales, las redes sociales y el gobierno electrónico. Tal como señala Marija Dalbello (2015, p. 205), la convergencia digital es el resultado de una serie de innovaciones que genera un mundo cada vez más interconectado de conocimientos, datos e información registrados; a la vez, la información constituye un elemento central en los procesos que sustentan la actividad o servicios de infraestructuras críticas de cuyo permanente funcionamiento depende el bienestar de las personas.

Todos estos factores generan una serie de desafíos a los Estados, y parte de las respuestas de los Estados a tales desafíos se orientan hacia la búsqueda de mayores grados de autonomía frente a los riesgos que genera la convergencia digital. Dicho proceso demanda mayores grados de libertad dando lugar a un dilema de seguridad, anclado en el antiguo y filosófico debate *hobbesiano*, que gira en torno a la tensión existente entre ambas dimensiones. Es decir, la visión de la utopía digital anclada en la libre circulación de la información en sociedades cada vez más conectadas ha revelado una amplia gama de problemas en cuanto a la seguridad y la defensa de las naciones. La información aparece como un activo estratégico y su uso como un factor de poder. Puede afectar las relaciones internacionales, puede ser una herramienta o medio para el logro de los intereses nacionales o bien un recurso para la paz o la guerra.

Todo este escenario descripto amerita ser objeto de reflexión desde el ámbito de la Defensa Nacional. Es por ello que este artículo se propone contribuir al debate académico, teórico y estratégico en torno a la Defensa Nacional en el ciberespacio desde una mirada holística y pragmática. No solamente es necesario entender y profundizar desde contribuciones generales mayoritariamente enraizadas en centros ubicados en países desarrollados o

CHRISTIAN L. GALASSO

Ingeniero en Electrónica (UTN-FRBB), docente del Posgrado en Análisis Operativo (ESOA). Investigador de la UNDEF, cat. C, director del grupo de I+D Soluciones Embebidas Aplicadas – UNDEF – Facultad de la Armada – ESOA.

MIGUEL ÁNGEL BANCHIERI

Ingeniero en Electrónica (UTN-FRBA), magíster en Ingeniería Biomédica (Universidad Favaloro) y profesor titular ordinario con dedicación exclusiva (UT.N-FRBB).

FRANCO CASPE

Ingeniero en Electrónica (UTN-FRBB), becario en PIDDEF 08/12. En 2017, trabajó como ingeniero en software para Hellastorm. En 2018, fue pasante IAESTE en Coimbatore, (India) en diseño de antenas.

MARTÍN DE PAZ

Estudiante de la carrera de Ingeniería Electrónica de la UTN-FRBB. Técnico Universitario en Electrónica 2018. Integrante del Grupo de Robótica y Simulación de la UTN FRBB. Investigador del grupo de I+D Soluciones Embebidas Aplicadas. UNDEF – Facultad de la Armada – ESOA.

Resumen

A continuación, se describe el diseño de un protocolo de comunicaciones que permite el intercambio de información entre una red de ordenadores de aplicación específica, que opera en tiempo real, y una PC comercial que

potencias industriales, sino que además es necesario construir una mirada crítica y constructiva desde la periferia, desde países en vías en desarrollo con las realidades propias de su coyuntura geopolítica.

En este camino, inicialmente se presentarán algunas contribuciones para entender de qué hablamos cuando hablamos de ciberespacio y establecer sus características y problemáticas de cara al debate teórico-estratégico que pretendemos. Seguidamente, se plantearán los límites de la convergencia digital frente a la soberanía nacional –o los límites de esta frente a la convergencia digital– para cerrar con una reflexión sobre estas cuestiones y la importancia de construir nuevas líneas de investigación desde la periferia.

El ciberespacio: nociones para una mirada político-estratégica

"La esfera digital ha penetrado profundamente nuestras vidas personales y a la sociedad en su conjunto", afirma Josepha Ivanka Wessels (2017) en un trabajo que se remite a un encuentro realizado en el Centro de Resolución de Conflictos Internacionales (CRIC) de la Universidad de Copenhague. Esta cuestión demarca una observación clara y atinada, "la era digital abre nuevos terrenos para la investigación de la paz y el conflicto" (p. 125).

Tal como afirma Manuel Castells (1996; 2007; 2009), vivimos en la era de la información, que comenzó con la introducción de la primera computadora personal en la década de 1970, iniciando la revolución digital. Esta época se caracteriza no solamente por la exacerbación hiperbólica de la información, sino por su capacidad de circular en redes, o, en otras palabras, el ciberespacio.

Encontrar una definición de ciberespacio no es una tarea sencilla. A la hora de abordar el fenómeno aparecen diversas definiciones que difieren en aspectos técnicos, políticos e incluso filosóficos. Por ejemplo, el Comité de Sistemas de Seguridad Nacional de los Estados Unidos lo define como un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de sistemas de información que incluye internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados (CNSS, 2015). Los famosos teóricos de la ciberguerra, Richard Clarke y Robert Knake (2010), afirmaban que diferentes generaciones piensan en ciberespacio de distinta manera, dando cuenta de

un fenómeno en movimiento, en constante transformación.

Joseph Nye Jr. (2010) lo entiende como un régimen híbrido único, hecho por el hombre, de características físicas y virtuales, conformado por los recursos tecnológicos electrónicamente interconectados de la informática. Algo que caracteriza al ciberespacio, según Nye, es su capacidad de traspasar las fronteras físicas. Sobre esta característica, el autor estructura la noción de "ciberpoder", al que define como la capacidad de un actor de lograr resultados deseados mediante el empleo de los recursos tecnológicos del ciberespacio, ya sea dentro del mismo ciberespacio –como un ataque de denegación de servicio– o en los otros ambientes operacionales –como podría ser interrumpir el suministro eléctrico de una estación empleando un virus informático.

Una contribución interesante para la definición del ciberespacio es el aporte de Martin Libicki (2009), el cual consiste en una aproximación por capas integradas verticalmente que permiten plantear una aproximación teórica y gráfica del ciberespacio. La propuesta de Libicki divide el ciberespacio en tres capas integradas. La primera capa, la "física", es la que se encuentra compuesta por todos los dispositivos técnicos o *hardware* tales como routers, cables, satélites, etc. La segunda capa, denominada "sintáctica", es la que se encuentra representada por el *software,* y es la capa que estructura, configura y controla la información. Finalmente, la tercera capa, que denomina "semántica", se entiende como la dimensión en la cual la información adquiere significado para los seres humanos.

A partir de las posibilidades tecnológicas que permiten dichos mecanismos lógico-digitales, se estructura una dimensión que articula la relación tanto entre seres humanos como de seres humanos con la infraestructura física. Incluso, se han originado núcleos de interacción, comercio, ocio, aprendizaje, entre otras cosas, puramente digitales. Así, podemos también considerar el ciberespacio como un ámbito digital de interacción humana:

> *Un ámbito digital de interacción humana, a través del cual se procesan distinto tipo de relaciones entre personas, grupos o Estados. Esta definición aquí propuesta, además de contemplar la naturaleza tecnológica del ciberespacio, nos permite avanzar en los aspectos político-estratégicos derivados de su uso, siendo la formulación de políticas específicas de seguridad y/o defensa una de sus muchas manifestaciones*
>
> (Gastaldi *et al*., 2018, p. 8).

De este análisis se desprende entonces un elemento que caracteriza al ciberespacio: la transversalidad. La transversalidad del ciberespacio puede abordarse de una forma dual o incluso tripartita, considerando las estruc-

turas físicas que dan lugar a su existencia y las características propias de su existencia como resultado de la interacción entre seres humanos (Castells, 2009). Ciertas dinámicas que ocurren en el ciberespacio pueden afectar directamente las estructuras y los dispositivos técnicos más allá de la gestión de las percepciones sociales, es decir, de sus usuarios. En otras palabras, las barreras entre la capa física y lógica-digital se han ido desdibujando, dando lugar a una serie de posibles acciones que permiten la influencia directa del mundo digital en el mundo físico o real, no solamente en los dispositivos técnicos, sino también en la vida personal de los individuos.

El optimismo del futuro –¿o del pasado?– anclado a las nuevas tecnologías de la comunicación, las posibilidades que internet brinda como tecnología abierta, colaborativa y democrática, y todas las nuevas oportunidades de la llamada cuarta fase de la industrialización, se encuentran así con su lado oscuro: los recientes escándalos que giraron en torno a WikiLeaks, Facebook y Cambridge Analytica han puesto de manifiesto una problemática severa en cuanto la disponibilidad, el acceso y la utilización de la denominada "Big Data" en la política y el surgimiento de nuevas amenazas y riesgos para las naciones y los individuos.

El dilema, sin embargo, no es aparentemente tan claro: la libertad y la vigilancia de la distribución de información sensible para los gobiernos puede ser identificada desde, al menos, dos perspectivas. La primera, cómo esa información sensible, al ser vulnerada estaba atacando no necesariamente a una infraestructura particular del sistema de poder de muchas naciones, sino que esa divulgación de información pone en jaque equilibrios intra e interestatales. La segunda, cuáles son los instrumentos y las estrategias necesarias para generar mecanismos de defensa frente a las nuevas vulnerabilidades que surgen a raíz de las transformaciones económicas y sociales estructuradas en base al ciberespacio.

El ejercicio del poder yace principalmente en la capacidad de los actores de enmarcar, priorizar y establecer agenda, influyendo directamente en la construcción de las percepciones de los ciudadanos con el mundo que los rodea. De allí surge la fuerza de internet como elemento de propaganda. Pero este poder no solo alcanza a los individuos que operan o usan la red, sino también a las comunidades de individuos políticamente organizados en un territorio dado: los Estados. Los Estados han encontrado en las operaciones cibernéticas un medio o herramienta para influir en otros Estados, de manera disruptiva, o mediante la degradación o el espionaje (Valeriano

et al., 2018). Así, a través del ciberespacio un Estado puede alcanzar sus objetivos políticos sin la necesidad de entrar en combate. En tal sentido, el componente ciber juega un rol estratégico en las relaciones internacionales. Tal afirmación la sostienen, por caso, Borges Gama Neto, Guedes de Oliveira y Vilar Lopes (2016), quienes plantean la necesidad de que, entrado ya el siglo XXI, las Relaciones Internacionales (RRII) deberían considerar un subcampo en la disciplina, denominado CiberRRII, o relaciones internacionales cibernéticas. Así, podemos considerar también la necesidad de avanzar en otros conceptos –además del ya largamente empleado ciberguerra–, como ciberpaz o ciberdiplomacia.

Sin embargo, no son solo los Estados los actores centrales de este escenario estratégico. También juegan roles significativos actores no estatales, ya sea un solo individuo –como el caso de Edward Snowden– u organizaciones, como pueden ser grupos hacktivistas –WikiLeaks o Anonymous– o grupos criminales y terroristas. Por ello, Joseph Nye (2010) correctamente señala que el ciberespacio se caracteriza por la dispersión del poder: en el ciberespacio existe una multiplicidad de actores que, empleando diversos recursos digitales, explotan vulnerabilidades para imponer su voluntad o influir en determinados eventos, como ha sido, por dar un ejemplo, la presunta intervención de Rusia a través de WikiLeaks en las últimas elecciones presidenciales de los Estados Unidos.

Incluso, surge la necesidad de reflexionar en torno a la capa física que hace posible las interacciones del ciberespacio. Dicha infraestructura implica necesariamente la activa participación de tecnologías estratégicas tanto virtuales como físicas. En este sentido, la cuestión de la autonomía, dependencia e interdependencia cobra un nuevo sentido, frente a elementos que no son neutrales ni libres, sino todo lo contrario; obedecen en última instancia a intereses de otros actores.

Los límites de la convergencia digital

Frente a una amplia gama de amenazas y riesgos que atentan contra la vida de las personas, los Estados organizan e instrumentan políticas con el fin de atender las preocupaciones que existen o se generan sociopolíticamente. En este sentido, cada país elabora e implementa políticas públicas que buscan dar respuesta a los riesgos y las amenazas que consideran fun-

damental atender. Tal como señala Mariano Bartolomé (2006, p. 133), no todos los Estados enfrentan las mismas amenazas o perciben como tales los mismos fenómenos ni valoran de la misma manera los bienes y/o valores que pueden ser afectados. Sin embargo, en un mundo hiperconectado, la información cobra un valor estratégico, y el permanente funcionamiento de las infraestructuras que permiten tal conexión se ha constituido en elemento vital para todos los Estados.

En este sentido, la soberanía se constituye en un concepto central en cuanto al ejercicio de poder del Estado, tanto en su interior como frente a los riesgos y amenazas que atentan contra la seguridad de sus miembros, sus infraestructuras y sus recursos. Aun así, el concepto soberanía conlleva también dificultad respecto a su definición, con distintas acepciones relacionadas con los derechos y obligaciones del Estado dentro y fuera de sus fronteras.

En general, el término soberanía se relaciona con el ejercicio de la autoridad por parte del Estado. Entre los primeros acercamientos teóricos a este concepto es preciso destacar a Thomas Hobbes, quien señala en el *Leviatán* que la soberanía es una forma de poder encarnada en el monarca, a quienes los hombres deben obediencia a través del contrato social. En el caso de Rousseau, es el ejercicio de la voluntad general.

Uno de los aportes más relevantes al pensamiento contemporáneo de la soberanía halla sus raíces en la propuesta de Jean Bodin (Andrew, 2011), quien dio lugar a la reflexión de la soberanía en el marco de la República, siendo esta perfectible pero la mejor de las alternativas posibles. La distinción realizada por el autor entre gobierno y soberanía es una piedra angular de su pensamiento, ya que el poder soberano recae en última instancia en el pueblo en una democracia, en una minoría en una aristocracia y en una persona en el caso de la monarquía. A grandes rasgos, la República es la estructura institucional moderna occidental en la cual se practica la acción política gubernamental.

Otro aporte que es importante considerar para el análisis de la soberanía es el presentado por Sassen (2010), quien enfatiza cómo el término ha sido modificado a lo largo del tiempo. La autora recuerda que en un primer momento la soberanía fue concebida como un atributo que poseía un individuo poderoso cuya legitimidad sobre el territorio descansaba en una autoridad divina o histórica, sea esta directa o delegada. Con la aparición del Estado-Nación, aparece la idea de soberanía exclusiva. Para la autora, la sobe-

ranía territorial (soberanía exclusiva) "supone la existencia de un acuerdo mutuo para el reconocimiento de una demarcación espacial de la autoridad política. En este sentido, exige un principio de equivalencia jurídica" (2010, p. 121). Esta idea, una vez finalizada la Segunda Guerra Mundial, abrió camino a una concepción de soberanía como voluntad del pueblo, estableciéndose como una de las condiciones de legitimidad política para los gobiernos.

Es destacable entonces cómo, desde el surgimiento de la idea de soberanía en el concierto internacional hasta la actualidad, diversos acontecimientos han ido erosionando lo categórico e excluyente de la soberanía nacional como una concepción meramente territorial, abriendo las puertas a la inclusión de nuevas acepciones. En palabras de Sassen (2010), la globalización tecnológica, de la mano de la digitalización global de mercados financieros (esto es el comercio a través de internet), ha transformado significativamente la autoridad del Estado-Nación, por lo que la autora nos invita a cuestionarnos respecto de si la soberanía o la territorialidad son hoy en día características de menor importancia en el sistema internacional.

Claro está que la soberanía brinda a los Estados no solo derechos sino también obligaciones que van de la mano de su ejercicio. La función clásica asociada a la soberanía ha sido la de proporcionar seguridad interna y externa a los habitantes de su territorio. En este sentido, hablar de soberanía entonces también es hablar de independencia o autonomía. Independencia de una entidad estatal para ejercer funciones de forma exclusiva sobre un territorio frente a cualquier otro Estado. Von Heinegg (2013) define esta autonomía como soberanía territorial, la cual contempla una forma de proteger a los Estados ante cualquier forma de injerencia por parte de sus pares.

Para Bauchner, por ejemplo, "la soberanía estatal es la entidad mediante la cual un territorio y una población se encuentran bajo el control de su propio gobierno y, a partir de la cual, posee la capacidad de entablar relaciones con otras entidades similares" (2000, p. 692). Este autor incluye, en el marco de su definición, la potestad y capacidad de vinculación internacional de la entidad que posee soberanía. Dada la ausencia de una autoridad central legítima, las relaciones entre los Estados son horizontales. Teniendo cada uno de ellos soberanía sobre un determinado territorio se espera, en la arena internacional, que se respete esa soberanía no interviniendo en los asuntos internos de otro Estado.

En este marco, cabe recordar la propuesta de Schmitt frente a la conceptualización de soberanía, que demuestra su profunda raíz política. La cons-

trucción de lo político y la soberanía se apoyan en la existencia de un otro. Para Schmitt, lo político alude a los conceptos de inclusión-exclusión, a partir de los cuales es posible diferenciar un nosotros, que se manifiesta en la constitución de un Estado, frente y en contraposición a los otros que pertenecen a otra unidad política (Marcos, 2004, p. 54). Sin embargo, los debates contemporáneos abren las compuertas de una amplia variedad de actores – y no-actores – de diferente naturaleza a la estatal que pueden poner en riesgo la soberanía nacional.

La construcción política de soberanía estructura un principio básico de la estatalidad acuñada por Schmitt en la frase *"Protego, ergo obligo"*. De esta forma, el ejercicio del poder soberano se apoya en la noción básica de protección frente a lo externo. Ahora bien, la forma de proteger y obligar surge a raíz de las especificidades propias del Estado en cuestión. Las percepciones y el establecimiento de prioridades de lo que es y no es una amenaza como construcción intrínsecamente política dan lugar a una amplia variedad de acciones posibles por parte de dicho Estado.

Dicha cuestión impacta directamente en cómo cada actor define sus políticas. En el caso de la política de defensa entendida como la acción política de una dimensión más abstracta identificada como "Defensa Nacional", no posee una definición salvo aquella concepción básica intrínsecamente vinculada al concepto de soberanía. La defensa de lo nacional es, en todo caso, las políticas destinadas a las preocupaciones que surgen en torno de la soberanía.

Es decir, así como existen diferentes percepciones de los fenómenos que pueden o no representar riesgos o amenazas, se pueden observar diferentes formas de dar respuesta ante fenómenos similares. La variedad de posibles aproximaciones de cada uno de los países demuestra una compleja red de interacciones y variables que intervienen generando un abanico de posibilidades que no pueden reducirse a una sola definición de lo que es Defensa Nacional. Es decir, no solamente hay diferentes riesgos y amenazas sino también distintas maneras en las que los países se enfrentan a ellos (Ocón, 2017).

Sin embargo, la defensa nacional como concepto es objeto de múltiples interpretaciones vinculándose a otras dimensiones como las de poder y autonomía. Hoy en día, difícilmente pueda plantearse que toda política de defensa se encuentra asociada solamente a los riesgos y amenazas. La proyección de poder y los intereses nacionales juegan un rol fundamental en la

construcción teórica, ideológica y política de la defensa nacional.

Aportes tales como los de Bartolomé (2006), Ole Wæver (2009) o Tarak Barkwai (2011) ponen de manifiesto los cambios históricos y conceptuales que han atravesado los debates y discusiones sobre la seguridad internacional, la paz y la guerra. Estos cambios, en muchos casos de carácter filológico, se ven reflejados en la construcción de políticas y diversas aproximaciones a la Defensa y la Seguridad Nacional en los países a lo largo de la historia, y consecuentemente a una amplia variedad de formas en las que se ejerce la soberanía.

La constante expansión de la esfera digital en las múltiples dimensiones de las sociedades, las economías, las culturas e incluso la política de las naciones ha dado lugar a una convergencia digital que no se encuentra liberada de dilemas estratégicos. Dicho fenómeno convive con la expansión de nuevas formas de riesgos, amenazas y vulnerabilidades.

La convergencia digital y el auge de la economía del internet y la sociedad de la información son todos aspectos positivos y optimistas, muchos los cuales fueron predichos en la declaración de Seúl para el Futuro de la Economía del Internet (OECD, 2008). Desde la perspectiva socioeconómica, internet se constituiría en un nuevo espacio económico y social que debía ser apoyado con medidas económicas específicas con el fin de apoyar su crecimiento y expansión resguardando el cuidado del consumidor. La interconectividad de los dispositivos y los usuarios constituyó un fin deseable y la libre circulación de la información un principio fundamental.

Estas ideas así habían sido plasmadas en los albores de internet, cuando el fundador de la ONG Electronic Frontier presentó en Davos en 1996 un documento titulado Declaración de Independencia del Ciberespacio, que expresaba

Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquella con la que la libertad siempre habla [...]

El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece de nuestras acciones colectivas [...]

En China, Alemania, Francia, Rusia, Singapur, Italia y los Estados Unidos estáis intentando rechazar el virus de la libertad erigiendo puestos de guardia en las fronteras del Ciberespacio [...] Debemos declarar nuestros "yos" virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos

(Barlow, 1996, pp. 241-242).

En sintonía con estos ideales, diversos países han incorporado el acceso a internet como un derecho fundamental en sus ordenamientos jurídicos, destacándose por ejemplo Finlandia por ser el primero en considerar el acceso a internet de banda ancha como un derecho constitucional de sus ciudadanos. Y a nivel internacional, la Organización de las Naciones Unidas también fomenta estos principios desde el año 2011 con la Declaración Conjunta sobre Libertad de Expresión e Internet.

Esta convergencia digital materializa así un nuevo desafío para la Defensa Nacional y la noción de soberanía. Desde una perspectiva (geo)política, se revelan dos aspectos fundamentales en lo que respecta a los límites de la convergencia. Por un lado, las implicancias y riesgos de la libre circulación de la información gracias a internet y, por otro lado, la tecnología y las infraestructuras que hacen posible internet.

En el mundo contemporáneo, donde existe una incremental estructuración de las dinámicas económicas y sociales en los espacios virtuales, se ha abierto las puertas a una serie de dinámicas novedosas en cuanto a los riesgos y las amenazas de las naciones y los individuos. Un *malware* puede no solamente hacer disfuncional un dispositivo, pueden incluso afectar la defensa y la economía de individuos, organizaciones y hasta naciones enteras.

Si la circulación de la información es lo que hace a las características de las sociedades y economías contemporáneas, dicha cuestión cobra valores inconmensurables. De esta forma, se crea la necesidad de resguardar y cuidar la información no solamente en sí misma, sino la privacidad de ella. El punto central es que la libre circulación de información no implica la anarquía de la información; sobre todo aquella que es relevante y fundamental para las naciones.

El caso de WikiLeaks revela una importante problemática en lo que respecta a los secretos de Estado en el mundo de la política y la seguridad internacional. En este sentido, lo que significó para muchos la defensa del principio de transparencia y libertad de la información, para muchos gobier-

nos implicó una severa amenaza que alteró importantes vínculos tanto para la política interna como externa de las naciones.

Tal como fue expresado, el ciberespacio plantea un nuevo desafío para la siempre cuestionada soberanía estatal. La naturaleza propia de este dominio resalta la importancia de políticas públicas que se aboquen a la búsqueda de mayores espacios de autonomía estatal en el mundo cibernético frente a la convergencia digital. La pregunta se erige imponente: ¿cuáles son los mecanismos para lograr mayor autonomía?

Luiijf, Besseling, Spoelstra y de Graaf (2011), en un interesante trabajo comparado, analizan diez estrategias nacionales de ciberseguridad, realizando observaciones respecto a las diferentes concepciones y abordajes nacionales. Así, estos autores se centraron en el análisis de Australia, Canadá, República Checa, Francia, Alemania, Japón, Holanda, Nueva Zelanda, Reino Unido y Estados Unidos a la luz de nueve interrogantes:

- ¿Cuál es la noción de ciberseguridad?
- ¿Cuáles son las amenazas percibidas?
- ¿Cuál es el alcance de las estrategias?
- ¿Existe una relación con otras estrategias nacionales?
- ¿Cuáles son los principios y los objetivos estratégicos?
- ¿Cuáles son las partes interesadas y cómo son abordadas?
- ¿Cuáles son las líneas de acción?
- ¿Se contemplan las amenazas emergentes?
- ¿Cómo son institucionalizadas las funciones nacionales?

Lo primero que destacan los autores no resulta particularmente sorprendente: no existe una definición aceptada y homogénea sobre ciberseguridad, a pesar de que podría ser beneficioso que así ocurriera. Cada Estado define la ciberseguridad de acuerdo a sus intereses particulares, de forma más o menos amplia. De hecho, solo cinco países definen explícitamente qué se comprende por ciberseguridad.

En segundo lugar, los autores observan que sí existe una relación entre las estrategias de ciberseguridad y otras estrategias nacionales, atendiendo a que la soberanía ciberespacial es otro atributo enmarcado entre las potestades estatales. De hecho, resulta particularmente interesante la vinculación entre la ciberseguridad y la infraestructura crítica, presente en la mayoría de las estrategias, a pesar de la falta de explicitación respecto a esa vinculación de acuerdo a los autores. En este sentido, parece clara la necesidad

de generar espacios de autonomía que permitan la protección cibernética de la infraestructura crítica de un Estado. La búsqueda de esta soberanía se presenta en las estrategias y es un enfoque necesario en tanto que la habilidad de un Estado para hacer frente a amenazas cibernéticas se relaciona directamente con su vulnerabilidad.

Este aspecto se refleja también en las amenazas percibidas, mencionando explícitamente siempre las amenazas a la infraestructura crítica y a la seguridad nacional. Luego de este acuerdo básico, sí los Estados se diferencian respecto a los riesgos que consideran, entre los que es posible enumerar sus habilidades defensivas, disrupciones sociales, pérdida de la confianza pública, ciberespionaje, cibercrimen y estancamiento económico. Estas amenazas, a su vez, pueden provenir de individuos, criminales, crimen organizado, terroristas, activistas y otros Estados.

Respecto a los objetivos, estos varían de acuerdo al punto de partida de cada estrategia. Así, es posible encontrar metas relacionadas con la prosperidad económica, la seguridad nacional o la defensa militar. Dadas las problemáticas que se presentan ante la expansión y auge del ciberespacio, se precisa dirimir políticamente sobre la tensión existente entre las ventajas y los riesgos de la convergencia digital y la necesidad de generar espacios autonómicos. Un cabal ejemplo de este dilema es mostrado en la respuesta político-estratégica que ha decidido Rusia: desarrollar un internet propio –Runet– que pueda funcionar independientemente de servidores extranjeros, con el propósito de defender al país de posibles ataques cibernéticos. Tal como lo expresó el senador Andrey Klishas del Partido Rusia Unida, "Estados Unidos tiene la capacidad técnica de desconectar a Rusia de los servidores principales; en otras palabras, internet dejaría de funcionar en Rusia, y como Estados Unidos cree que no tiene límites cuando se trata de sus intereses nacionales, Rusia como Estado soberano debe dotarse de los recursos técnicos para contrarrestar esas amenazas (France24, 18/05/2019). La agencia de noticias rusa, Sputnik, tituló el acontecimiento de la siguiente manera: "Se acabó el dominio de Estados Unidos: Rusia proclama la 'independencia' de su internet" (Sputnik, 17/04/2019). Este caso muestra cabalmente lo que queremos señalar: en defensa de la soberanía nacional, la búsqueda de autonomía en las infraestructuras de internet genera una preocupación creciente entre los Estados, y la convergencia digital encuentra así sus propios límites.

Pero, por otra parte, también es importante el recorrido, o la traza, de los flujos de información que habilitan estas infraestructuras. En este análisis,

Burzai (2014) estudia las conexiones de la Argentina con el mundo a través de internet y encuentra que toda conexión de datos que sale del país pasa el 81,05% por Estados Unidos primero, el 17,43% por Francia, y el 1,52% de las conexiones atraviesa en primer término Italia. Esto indica, tal como explica Burzai, que en el ciberespacio las fronteras de Argentina difieren de las fronteras físicas:

Mientras que en el espacio geográfico Argentina limita con cinco países: Bolivia, Brasil, Chile, Paraguay y Uruguay, en el ciberespacio, a través de Buenos Aires como mayor punto de conexión internacional, limita con tres: Estados Unidos, Italia y Francia [...] Solamente después de pasar por alguno de estos países se podrá llegar a cualquier otro país del sistema mundo (2014, p. 90).

Burzai concluye que la supuesta red descentralizada que constituye internet es en realidad un espacio altamente jerarquizado, que da lugar a nuevos centros y periferias:

Se pone en evidencia que los países centrales están entre todos los países periféricos, y que ninguno de estos últimos pueden limitar entre sí. Cualquier conexión entre Argentina y Estados Unidos se realizará de forma directa, pero entre Argentina y otro país latinoamericano la conexión estará mediatizada por la realización de escalas en puntos de control ubicados en los países centrales (2014, pp. 90-91).

De este modo, es posible observar que el ciberespacio está atravesado por relaciones de poder, y que el control o dominio de los nodos de información y la infraestructura física cumple un papel crítico. Los países periféricos, en este dominio, poco pueden hacer. El desafío entonces pareciera ser cómo ganar autonomía –y soberanía– frente a la dependencia.

Al mismo tiempo, la infraestructura física que hace posible la circulación del flujo de información revela otra problemática. Los cables submarinos, los *routers* centrales y hasta la tecnología satelital se encuentran en manos de empresas privadas de origen extranjero. Más allá de la relación Estado-empresa de cada una de estas, se pone de manifiesto un dilema estratégico.

Finalmente, es preciso mencionar las acciones previstas en las distintas estrategias: medidas de seguridad activas/dinámicas; concientización y capacitación; políticas adaptables al riesgo; continuidad y planes de contingencia; protección de la infraestructura crítica; protección criptográfica; operaciones de ciberdefensa; desarrollo económico; educación; ejercicios; manejo de crisis respecto a la infraestructura crítica; intercambio de información; inteligencia; colaboración internacional; desarrollo de conocimien-

to; legislación; estándares de seguridad; capacidad de detección; capacidad de respuesta; protección de la privacidad; promoción de una convención contra el cibercrimen; protección de la infraestructura no critica; asociación público-privada; reducción de la motivación y capacidades de los adversarios; investigación y desarrollo; resiliencia; protocolos y software; etc.

Reflexiones finales: desafíos desde la periferia y agenda de investigación

Cuando Alvin y Heidi Toffler (1994) anunciaban la llegada de una tercera ola, y de cómo esta iba a impactar en las guerras del futuro, pensaron en un "mundo trisecado", un mundo dividido en "tres civilizaciones tajantemente separadas, en contraste y competencia: la primera, simbolizada por la azada, la segunda por la cadena de montaje y la tercera por el ordenador" (p. 41). Esta nueva civilización de la que hablaban tales autores iba a reproducir en su interior relaciones de poder, así como a definir nuevos centros y periferias. La competencia mencionada por la hegemonía mundial claramente iba a caer en manos de los países de la tercera ola. No solo en términos de dominio de la infraestructura cibernética sino también el lugar que los países ocupan en la transferencia de la información revela posiciones claves en el sistema internacional y las posibilidades de situarse en algún extremo del clivaje autonomía-dependencia.

Los cambios tecnológicos de los que hablamos antes nos llevan asimismo a pensar si podemos seguir entendiendo la Defensa Nacional de la misma forma que en el pasado. En este mundo trisecado, pero a la vez articulado cibernéticamente, se plantean desafíos a la noción de soberanía nacional, a la cual la defensa contribuye. Un mundo en el que coexisten elementos tradicionales de poder en los ambientes tradicionales –agua, tierra, aire y espacio– con los elementos novedosos del poder cibernético que atraviesa dichos espacios, con un entorno propio de naturaleza virtual, pero a la vez físicamente anclado. Así, en este mundo se ensamblan diferentes modos de ejercicio del poder y riesgos y amenazas de variada naturaleza. La soberanía es lo que era, pero es también algo nuevo. En un plano, los Estados despliegan su soberanía sobre elementos territoriales; en otro plano, en el de la convergencia digital, es prácticamente imposible ejercerla. Así, podemos proponer que, en este nuevo mundo trisecado, coexisten diversas fórmulas

soberanas.

La era ciber nos lleva entonces a replantear viejos términos y conceptos. Siendo la soberanía estatal un interés vital a ser garantizado por la defensa nacional, se observa entonces la urgencia de establecer nuevas líneas de investigación en torno a esta actividad. El ejercicio de la defensa nacional requiere tomar nota de la información como un activo estratégico. Tal como expresaban Alvin y Heidi Toffler, "no se trata simplemente de una cuestión de información sobre el campo de batalla o de ataques tácticos a las redes de radar o telefónicas del otro bando, sino de una potente palanca capaz de alterar decisiones de alto nivel del adversario" (1994, p. 201). En otras palabras, el desafío central no está en la adquisición, procesamiento, distribución y protección de la información de los sistemas militares, sino en su empleo estratégico.

Las guerras 4.0 tal vez puedan librarse sin arrojar una sola bomba, sin disparar un fusil, e incluso, sin lanzar un virus informático contra los sistemas de información del enemigo; esto es, sin la necesidad de entrar en combate, solo empleando la información en forma estratégica para alcanzar los objetivos nacionales. En este marco, la Defensa Nacional adquiere un nuevo significado y es tarea de nosotros, los investigadores en la materia, dilucidarla.

En conclusión, los estudios y trabajos de Defensa Nacional deben ponderar:

- Que la arquitectura de todo el sistema de información posee alcance global, trasciende fronteras en el marco de la convergencia digital, y aun así, es gestionada por privados y unos pocos Estados.
- Que los países periféricos, o en vías de desarrollo, se encuentran con desigualdades estructurales y de infraestructura tecnológica necesaria para garantizar la defensa del interés nacional frente a los riesgos y amenazas que pueden presentarse en el mundo cibernético.
- De esta manera, frente al dilema autonomía-dependencia se pueden hallar caminos intermedios por medio de la cooperación internacional y el resguardo de áreas de influencia.
- Que la soberanía se expresa en múltiples dominios y de diferentes modos en cada uno de ellos y que se requiere un ejercicio intelectual y un debate académico para reinterpretar el concepto a la luz de los nuevos fenómenos y dinámicas.

Por último, resolver la tensión libertad-seguridad exige abrir una nueva

agenda de investigación si es que la ciencia proyecta apoyar de algún modo la acción política. Como sabemos, dicha dicotomía no es nueva, siempre ha existido y la manera en que los Estados han tratado de resolverla ha variado de la misma forma en que se han modificado las sociedades, el sistema mundo y los modelos económicos a lo largo de la historia.

Bibliografía

Bauchner, Joshua S. (2000). State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate. *Brooklin Journal of International Law*, 689-722.

Bartolomé, Mariano (2006). *La Seguridad Internacional post 11S: situación, debates y tendencias.* Buenos Aires: Instituto de Publicaciones Navales.

Barwaki, Tarak (2011). From War to Security: Security Studies, the Wider Agenda and the Fate of the Study of War. *Millennium*, 39 (3), 701-716.

Barlow, J. P. (2009). Declaración de independencia del ciberespacio. *Periférica Internacional. Revista para el análisis de la cultura y el territorio,* 1 (10), 241-242. Disponible en https://revistas.uca.es/index.php/periferica/article/view/943

Borges Gama Neto, R., Guedes de Oliveira, M. y Vilar Lopes, G. (2016). *Relações Internacionais Cibernéticas (CiberRi). Oportunidades e Desafios para os Estúdios Estratégicos e de Segurança Internacional.* Recife: Editora UFPE.

Burzai, Gustavo (2014). Fronteras en el ciberespacio: el nuevo mapa mundial visto desde Buenos Aires (Argentina). *Cuadernos de Geografía: Revista Colombiana de Geografía,* 23 (2).

Burzai, G. y Toudert, D. (2004). *Cibergeografía: Tecnologías de la información y las comunicaciones (TIC) en las nuevas visiones espaciales.* Mexicali, Baja California: Universidad Autónoma de Baja California.

Castells, Manuel (1996). *The Rise of the Network Society.* Oxford: Blackwell.

Castells, Manuel (2007). Communication, Power and Counter-power in the Network Society. *International Journal of Communication,* 1, 238-266.

Castells, Manuel (2009). *Comunicación y Poder.* Traducción de María Hernández. Madrid: Ed. Alianza.

Clarke, Richard y Knake, Robert (2010). *Cyberwar. The next threat to national security and what to do about it.* Washington DC: Harper Collins.

Dodge, Martin y Kitchin, Rob (2001). *Mapping Cyberspace*. London: Routledge.

Dalbello, Marija (2015). Digital Convergence: The past in the present. En Spence Richards, P. et al. (eds.) *A History of Modern Librarianship: Constructing the Heritage of Western Cultures.* California: Libraries Unlimited Ed.

Gastaldi, Sol 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.

von Heinegg, Wolff Heintschel (2013). Territorial Sovereignty and Neutrality in Cyberspace. *Naval War College International Law Studies*, 89, 123-156.

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

Marcos, Dolores (2004). Acerca de los conceptos de política y soberanía. En Schmitt, Carl y Hobbes, Thomas, *Foro Interno*, 45-58.

Luiijf, H. A., Besseling, K., Spoelstra, M., & de Graaf, P. (2011). Ten National Cyber Security Strategies: A Comparison. En S. Bologna, B. Hämmerli, D. Gritzalis, & S. Wolthusen, *Critical Information Infrastructure Security.* La Haya: Springer-Verlag Berlin Heidelberg, pp. 1-17.

Mayer, Marco, Niccoló de Scalzi, Martino, Luigi y Chiarugi, Iacopo (2013). International Politics in the Digital Age: Power Diffusion or Power Concentration? Paper review and adaptation of the first version presented by the authors in the *XXVIIth SISP Conference.*

Mueller, Milton (2004). *Ruling the Root: Internet Governance and the Taming of Cyberspace.* MIT Press.

Nye, Joseph S. (2010). *Cyber power.* Cambridge: Bedfer Center for Science and International Affairs.

Ocón, Alfredo Leandro (2017). Hacia una Estrategia Nacional de Defensa y Seguridad. En Academia Nacional de Ciencias Morales y Políticas, *Las Políticas de Defensa Nacional en el siglo XXI.* Buenos Aires: ANCMYP.

Sassen, S. (2010). *Territorio, autoridad y derechos. De los ensambles medievales a los ensambles globales.* Buenos Aires: Katz.

Segal, Adam (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: Public Affairs.

Toffler, Alvin y Heidi (1994). *Las guerras del futuro.* Barcelona: Plaza & Janés Editores.

Valeriano, Brandon, Jensen, Benjamin y Maness, Ryan (2018). *Cyber strategy. The evolving character of power and coercion.* Oxford: Oxford University Press.

Wessels, Josepha Ivanka (2017). Introduction: The Digital Age Opens Up New Terrains for Peace and Conflict Research. *Conflict and Society,* 4 (1), 125-129.

Wæver, Ole (2004). Paz y seguridad: dos conceptos y su interrelación. En Guzzini, Stefano y Jung, Dietrich (eds.) *Análisis contemporáneo de seguridad e investigación para la paz en Copenhague.* Londres: Routledge.

Otras fuentes y recursos

OECD (2008). Shaping the Policies for the Future of the Internet Economy, disponible en http://www.oecd.org/sti/40821707.pdf

Committee on National Security Systems (2015). *Committee on National Security Systems (CNSS) Glosary*, disponible en https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

France24 (18/05/19). La red de Internet se estrecha en Rusia. Disponible en https://www.france24.com/es/20190517-en-foco-rusia-internet-regulacion

Sputnik (17/04/2019). Se acabó el dominio de Estados Unidos: Rusia proclama la "independencia" de su internet. Disponible en https://mundo.sputniknews.com/rusia/201904171086763827-rusia-introduce-la-ley-de-estabilidad-del-segmento-ruso-de-internet/