Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM
Vol. XXX, N. 1 (2020), pp. 125-149

LA CONTRIBUCIÓN DE LA CIBER-RESILIENCIA AL PODER NACIONAL

Arturo GARCÍA HERNÁNDEZ
Centro de Estudios Superiores Navales (CESNAV), México

RESUMEN

El ciberespacio es un mundo virtual donde se realizan todo tipo de operaciones que requieren la correcta comunicación entre computadoras y personas. Por ello, una falla en este dominio virtual puede poner en riesgo las aspiraciones y objetivos de una nación.

La historia ha dejado claro que no existe la ciberseguridad al cien por ciento, sin importar la estrategia preventiva seguida. Ante la inevitabilidad de sucesos adversos en el ciberespacio, la capacidad de resistirlos y continuar adelante, es decir, su resiliencia o Ciber-Resiliencia (CR), es fundamental en la estrategia inherente a la defensa nacional.

Un país resistente y adaptable ante ataques en el ciberespacio, aun siendo víctima de uno, dará como resultado que se mantenga la consecución de los objetivos nacionales. El presente documento es complementario a otras visiones en torno al concepto de ciberseguridad, las enriquece y las replantea.

Palabras clave: seguridad nacional, defensa nacional, poder nacional, poder suave, poder duro, ciberpoder, ciberespacio, ciberseguridad, ciber-resiliencia.

THE CONTRIBUTION OF CYBER-RESILIENCE TO NATIONAL POWER

ABSTRACT

Cyberspace is a virtual world where all kinds of operations are carried out that require correct communication between computers and people. Therefore, a failure in this virtual domain can jeopardize the aspirations and objectives of a nation.

History has made it clear. There is no one hundred percent cybersecurity, regardless of the preventive strategy followed. Faced with the inevitability of adverse events in cyberspace, the ability to resist them and continue forward, in other words, their resilience or Cyber-

Resilience (CR), is fundamental in the strategy inherent to national defense.

A resistant and adaptable country to the attacks in cyberspace, even if it is a victim of one, will result in the achievement of national objectives being maintained. This document is complementary to other views around the concept of cybersecurity, enriches and rethinks them.

Keywords: National security, national defense, national power, soft power, hard power, cyber power, cyberspace, cybersecurity, cyber-resilience.

A. INTRODUCCIÓN

Los ataques en el ciberespacio son cada vez más frecuentes, con mayor intensidad y complejidad, como lo muestran las estadísticas publicadas en el mundo (Fire Eye, 2021).

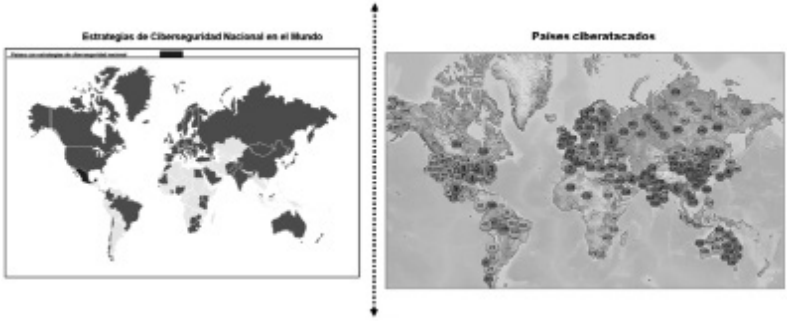
Romero Galicia (2018) elaboró una reseña sobre esta problemática y sobre las estrategias nacionales de ciberseguridad que han sido adoptadas por diversos países.

De manera particular ese artículo, basado en su tesis doctoral, hace una descripción de lo que debería contener una estrategia para México.

Lamentablemente, no importa la estrategia preventiva que se siga, siempre existirá la posibilidad de ser atacado exitosamente, lo que no significa que las estrategias de ciberseguridad no sean necesarias, siempre lo son, sobre todo para prevenir ataques y actuar inmediatamente; no obstante, muchas carecen de elementos de resiliencia.

En la siguiente figura se muestran los países con una estrategia nacional de ciberseguridad, la cual se contrasta con una identificación de los ciberataques de que los países han sido víctimas en los últimos años:

Figura 1. Países con ciberestrategia *vs.* países ciberatacados



Elaboración propia basada en (Romero G., 2018) y (CSIS, 2020).

Un ejemplo reciente de este problema es el ataque a gran escala que sufrieron los Estados Unidos de América:

"The Cybersecurity and Infrastructure Security Agency (CISA) is aware of compromises of U.S. government agencies, critical infrastructure entities, and private sector organizations by an advanced persistent threat (APT) actor beginning in at least March 2020. This APT actor has demonstrated patience, operational security, and complex tradecraft in these intrusions. CISA expects that removing this threat actor from compromised environments will be highly complex and challenging for organizations" (CISA, 2020:1).

(La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) está consciente de los compromisos de las agencias gubernamentales de EUA, las entidades de infraestructura crítica y las organizaciones del sector privado de una amenaza avanzada persistente (APT) por parte de un actor a partir de al menos marzo de 2020. Este actor de APT ha demostrado paciencia, seguridad operacional y comercio complejo en estas intrusiones. CISA espera que será muy complicado y desafiante para las organizaciones eliminar a este actor de amenazas de entornos comprometidos) (CISA, 2020:1).

Este país se encuentra en los primeros lugares de índices de ciberseguridad (ITU, 2020); además, cuenta con estándares, guías,

instituciones, personal y presupuestos dedicados a este rubro (Gobierno EUA, 2020). Dadas estas características, se puede considerar como una potencia mundial en ciberseguridad.

No obstante, muchas de sus organizaciones gubernamentales y otras empresas de importancia sistémica que tenían fuertes controles preventivos fueron atacadas mediante la irrupción en un sistema en su cadena de suministro, provisto por una empresa de confianza, precisamente relacionada con herramientas de ciberseguridad.

Esta fue una de las razones por lo que nadie sospechó que uno de sus productos de software contuviera un código malicioso, el cual se distribuyó ampliamente. Organizaciones como la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EUA (CISA, por sus siglas en inglés), el Departamento de Estado, el Departamento del Tesoro, e incluso empresas como Microsoft y Fire Eye, entre otros más, fueron víctimas del ataque.

De las afectaciones que se dieron a conocer se sabe que los agresores pudieron ver las entrañas de algunos programas de Microsoft y de Fire Eye, que son ampliamente utilizados en el mundo. Al momento de redactar este artículo solamente se sabe que algunas organizaciones del gobierno de EUA utilizaban dichas herramientas, pero no se tiene información del impacto concreto ni del autor de dicho ciberataque1, el cual tomó bastante tiempo en instrumentarse y contó con amplios recursos materiales y humanos. Dadas estas características, se intuye que fue respaldado por algún gobierno hostil a los intereses de EUA, como pudieran ser organizaciones en Rusia, Corea del Norte o Irán.

Así, se puede contemplar que siempre habrá alguna manera de perpetrar un ataque exitoso. En el ciberespacio cualquier elemento en la cadena de suministro (de servicios, aplicaciones, infraestructura, etc.) es susceptible de ser vulnerado para alcanzar a otros elementos de la cadena. Como lo menciona Nye en su artículo Deterrance and Dissuasion in Cyberspace (p. 50) “no existe una garantía de la seguridad (en el ciberespacio)”, y que siempre habrá formas de superar las barreras.

Con base en esta falta de garantía y, por tanto, la inevitabilidad de un ciberataque exitoso que supere los controles informáticos establecidos, la resiliencia resulta de vital importancia en este dominio virtual. Esto indudablemente afecta al Poder Nacional.

Como lo indica Joseph Nye en su libro The Nature of Power, el poder ahora es más difuso, sobre todo gracias a las tecnologías de la información, y ahora se encuentra distribuido en diferentes naciones. Esto genera que el poder ya no solamente esté concentrado en países específicos; la asimetría del poder es una realidad (2011).

En las siguientes secciones se define el concepto de resiliencia, con el propósito de integrarlo y enriquecer las acepciones de seguridad nacional, defensa nacional y poder nacional. Se considera que la comprensión de estos términos es esencial para describir correctamente su integración.

B. CONCEPTO DE RESILIENCIA

El Diccionario de la Lengua Española señala que la palabra "resiliencia" proviene del latín "resilïre", que significa "volver atrás, volver de un salto, resaltar o rebotar". Este vocablo ha sido utilizado en diferentes disciplinas, como en el uso de materiales, ecología, planeación urbana, por mencionar algunas.

Originalmente, en el entorno de los materiales la resiliencia hacía referencia principalmente a la propiedad de absorber la fuerza exterior que se aplicaba a dicho material y que permitía que recuperara su forma después de haber sido doblado o comprimido (Dupont, 2019).

En el ámbito del ciberespacio se aprovechó este concepto para describir una situación similar (ciber-resiliencia), esto es, seguir adelante ante un incidente que afecta o daña la seguridad de la información.

Para efectos de este artículo se utilizará la definición de elaboración propia basada en la literatura consultada: "Ciber-resiliencia

es la capacidad de anticiparse, soportar y recuperarse, parcial o totalmente ante un ciberataque, a fin de proveer continuamente bienes y servicios hasta alcanzar un nuevo equilibrio, bajo condiciones diferentes al estado inicial".

Esta definición apoyará para la mejor comprensión del término y repercusiones en otros campos, pues incluso en esferas puramente tecnológicas no es entendido en su totalidad. Por ejemplo, su aplicación al mundo del ciberespacio hace énfasis en la provisión continua de los bienes y servicios basados en tecnologías de la información; sin embargo, como se puede advertir en la definición, el verdadero sentido de la resiliencia se basa en el retorno a un nuevo estado (y no precisamente al original) donde se presentó el incidente, elemento que no está presente en algunas definiciones.

Esto es de particular relevancia, pues no se está hablando de "continuidad de negocio", por ejemplo, el cual precisamente busca regresar a un estado inicial idéntico al previo al incidente. En términos de la CR esto no es precisamente lo que ocurrirá, pues se seguirán suministrando los bienes y servicios, pero bajo un nuevo escenario (o equilibrio).

De esta manera, la definición también hace énfasis en su carácter "evolutivo y adaptativo" y no solamente preventivo, como en ocasiones lo quieren entender algunas organizaciones, sobre todo compañías comerciales que desean transmitir el mensaje de "resistir un ciberataque". Si bien la resiliencia pudiera tener una connotación preventiva, ésta no es su naturaleza.

Ello corresponde a las etapas del desarrollo de un trastorno conforme fue establecido por la Academia Nacional de Ciencias (NAS, por sus siglas en inglés): Planear y Preparar, Absorber, Recuperar y Adaptar (National Academies Press, 2012).

Siguiendo esta clasificación, proponemos establecer los tipos de resiliencia identificados:

Tabla 1: Tipos de Ciber-Resiliencia		
Tipo de Ciber-Resiliencia	**Etapa del trastorno**	**Descripción**
Preventiva	Planear/ Preparar	Previene que ocurra un incidente y parcialmente planea qué hacer ante ciertos escenarios posibles. Es el uso más común del término.
Reactiva	Absorber/ Recuperar	Empleada en cuanto ocurre un incidente y, en el mejor de los casos, aplicando lo planeado para algún escenario.
Inteligente	Adaptar	Toma en cuenta la adaptación y evolución de la organización.
Elaboración propia con base en National Academies Press, 2012.		

Si bien todos los tipos de CR tienen por objetivo mitigar el impacto de un incidente, conforme a la naturaleza del propio concepto, solamente se logra una aplicación efectiva e integral en la categoría "inteligente". Muchas organizaciones se valen parcialmente de lo que ellas entienden (o lo que les venden) por CR, siguiendo solamente estándares preventivos y/o reactivos, sin alcanzar un nivel inteligente adaptativo ante cualquier circunstancia adversa.

Esta precisión resulta importante, ya que la interpretación correcta del concepto facilitará la comprensión de su relación con la seguridad y defensa nacional que se expone a continuación.

C. CONCEPTOS DE SEGURIDAD NACIONAL

Seguridad nacional y defensa nacional se han llegado a confundir e incluso a utilizar de forma intercambiable, lo cual es un error, pues son concepciones que, si bien tienen un fin común, son diferentes en su aplicación.

Como lo indica Soto Silva (2009) en su artículo La Defensa Nacional de la A a la Z, la distinción de estos términos es indispensable para entender su naturaleza e interrelación, más para esferas civiles, ya que sobrepasan el ambiente puramente militar, son de carácter nacional y requieren la comprensión por toda la sociedad para su efectiva operación.

Esto también lo señala Cámez Meillón al comentar: "[…] contrasta con lo que acontece en el ámbito civil en México, en el que se percibe la ausencia del debate, la discusión e incluso la sola mención del término "poder nacional".

Por ejemplo, el término no se menciona en el discurso político, lo que conlleva a que sea un término poco sociabilizado y, por tanto, con limitado potencial para su impulso en pro del desarrollo del país" (2020:3).

1. Seguridad Nacional

La definición oficial de Seguridad Nacional es la que aparece en el Artículo 3 de la propia Ley de Seguridad Nacional de México (LSN), 2005: "[…] se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano".

No obstante, esta definición parece limitada, ya que se refiere más a un estado o sentimiento de paz. Por ejemplo, en el Glosario de Términos Unificados de la Secretaría de Marina (SEMAR) y la Secretaría de la Defensa Nacional (SEDENA) de 2018 se define a la Seguridad Nacional como: "Condición necesaria que proporciona el Estado para garantizar la prevalencia de su integridad territorial, independencia, soberanía, estado de derecho, su estabilidad política, social y económica y la consecución de sus Objetivos Nacionales" (p. 23).

Esta misma concepción es la que se puede identificar en otras definiciones oficiales de otros países. Dussán Hernández (2005) recopiló varias, que convergen en que es una "condición", y no necesariamente un conjunto de acciones, para la consecución y salvaguarda de los objetivos nacionales, que son los bienes tutelados por la seguridad nacional.

En este sentido, resulta valioso reflexionar sobre la definición de seguridad nacional que comparte Thiago Cintra en el compendio Seguridad Nacional, Poder Nacional y Desarrollo: "[…] la garantía que, en grado variable, es proporcionada a la nación, principalmente por el Estado, a través de acciones políticas, económicas, psico-

sociales y militares para que una vez superados los antagonismos y presiones se puedan conquistar y mantener los Objetivos Nacionales Permanentes" (p. 54).

A continuación se analizan algunos de los términos utilizados en la definición anterior, que servirán para encuadrar ámbitos en el ciberespacio, materia de este artículo:

- *Garantía en grado variable: Expresa la condición y anhelo del concepto.*
- *Acciones políticas, económicas, psicosociales y militares: Hace una clara distinción entre ese anhelo y las acciones a instrumentar en consecuencia. Asimismo, se deja entrever que, para lograr dicho anhelo, se aprovecharán las herramientas con las que cuenta el poder nacional. Posteriormente se verá que el ciberpoder es un componente del poder nacional.*
- *Superación de antagonismos y presiones: El hecho de "superar" da una entrada clara a que no sólo se previene, mitiga o nulifica al ente antagónico. La resiliencia es una forma de superación. Esta es la característica muy importante a considerar para la relación entre el concepto de seguridad nacional y la CR.*

2. Defensa Nacional

Por su parte, la Defensa Nacional representa a las acciones concretas que se deben realizar para la consecución de la misión de la seguridad nacional.

En el Glosario de Términos Unificado indicado anteriormente así se define a este concepto: "Función permanente del Estado mexicano que conlleva un conjunto de acciones, recursos y medios que adopta y dispone para garantizar su integridad, independencia y soberanía, así como prevenir y eliminar los antagonismos que procedan del ámbito externo e interno y preservar la estabilidad y el desarrollo nacional" (p. 7).

Cintra (1991:56) indica claramente que "la seguridad es una condición; defensa es un acto directamente relacionado con un tipo de amenaza". Esta diferencia es fundamental para la correcta com-

prensión de ambos conceptos, donde uno, la seguridad, engloba al de defensa.

Al respecto, Dussan Hernández (2005) remarca la diferencia entre estos dos términos e indica: "[la seguridad nacional] es un concepto más amplio que el de la defensa nacional, puesto que también abarca el desarrollo socioeconómico institucional y cultural… [la defensa nacional] es un concepto más restringido que la seguridad, ya que sólo se refiere al mantenimiento de las condiciones que le permitan al país asegurar sus intereses primarios, ante posibles amenazas o acciones del exterior".

Siguiendo esta línea de pensamiento se pudiera entender que la defensa es de naturaleza únicamente preventiva.

Si bien esto es parcialmente cierto, la defensa nacional también implica una parte reactiva cuando un antagonista ataca a la nación. Por tanto, la preservación de la estabilidad y desarrollo nacional involucra la ejecución de acciones, las cuales se hacen con el Poder Nacional.

En términos del ciberespacio, el que suceda un ataque exitoso, como se describió al inicio de este documento, no significa una derrota total de una nación ante un antagonista, más bien indica que se deben tomar acciones de defensa reactivas para contener los daños, con el fin de preservar los objetivos nacionales.

Además, en este campo virtual no existe una acción clara y concreta de cuándo inicia o termina un ataque cibernético, y por tanto la resiliencia no tendría un inicio ni un final concluyente, todas sus acciones son parte de lo que constituye la defensa nacional. La CR implica acciones, la pasividad no es precisamente un elemento de resiliencia.

Del mismo modo, hasta hoy en día no se ha presentado una declaración expresa de guerra en el ciberespacio (o también llamada "ciberguerra"), sólo han habido conflictos que, aunque han escalado, no han llegado a una declaración de guerra (Singer y Friedman, 2014). Si bien muchos de los conflictos en el ciberespacio han sido

precursores de enfrentamientos armados en el mundo físico, todos los ciberataques caen en una zona gris.

Nye, en su documento Deterrance and Disuassion in Cyberspace señala esto mismo: "In the classic duality between war and peace, they fell into a gray zone […] Resilience is essential both to reduce an adversary's benefits of attacking critical infrastructure and to assure that cyber and noncyber military response options are available for retaliation" (p. 48).

(En la clásica dualidad entre guerra y paz, cayeron en una zona gris […] La resiliencia es esencial tanto para reducir los beneficios del adversario al atacar la infraestructura crítica como para asegurar que las opciones de respuesta cibernética y no cibernética militar estén disponibles para represalias) (p. 48).

Soto Silva hace un señalamiento similar al indicar que: "[…] la solución del conflicto asume alguno de sus dos tipos básicos, crisis o guerra, aunque es perfectamente posible que uno devenga en el otro sin solución de continuidad. De acuerdo con la forma en que se han venido desarrollando los acontecimientos en el mundo actual, lo más probable es que la solución que se generará con mayor probabilidad a un conflicto sea la crisis".

Más adelante, Soto Silva define una crisis de la siguiente manera: "Es una forma de solución de un conflicto de intensidad limitada, que involucra a actores del sistema internacional, en el que se trata de lograr ciertos objetivos mediante presiones o negociaciones sin llegar al enfrentamiento o uso generalizado de la fuerza" (p. 298).

Esto es exactamente lo que se ha visto en el ciberespacio con los ataques informáticos sucedidos hasta el momento. En este punto se puede relacionar directamente a la resiliencia con el concepto de seguridad nacional, en términos de que apoya a la consecución de los objetivos nacionales; y a la defensa nacional, en virtud de que la resiliencia es un instrumento concreto que coadyuva en esa protección ante la presencia de antagonismos que ponen en riesgo los bienes tutelados.

En el siguiente apartado se describe la relación de la resiliencia con el Poder Nacional, parte medular de este artículo.

3. Poder Nacional

El término "poder" es amplio y con múltiples acepciones. Comenzando con una básica, se puede definir simplemente como "tener expedita la facultad o potencia de hacer algo" (Real Academia Española, 2020). De hecho, este mismo término aparece con decenas de significados en ese mismo diccionario, muchas de las cuales aluden a un acto de imposición de una voluntad. Esta connotación negativa es lo que ha derivado en su entendimiento de violencia por algunas esferas.

En la tesis doctoral de Cámez Meillón (p. 42) se hace referencia a una serie de definiciones de "poder" con base en varios autores, en las cuales se puede identificar claramente este tipo de concepción. Si a este término se añade la palabra "nacional", entonces se podría interpretar que sería la capacidad de un Estado-Nación para imponer su voluntad contra toda resistencia, tanto del pueblo mismo como de los antagonistas externos, lo cual es claramente parcial y, peor, fuera de contexto.

Esto es erróneo totalmente, como lo señala en el mismo documento: "Sin embargo, las anteriores aproximaciones requieren evolucionar a través de la complementación con el poder del ser humano hacia los objetos y otros seres, que al final se incorporan también en la lógica de las relaciones sociales desde la perspectiva sistémica del poder nacional sostenible" (*Ibid.*, p. 57).

Es exactamente este sentido al que refiere Cámez Meillón, en el que se concibe la aplicación del poder a la resiliencia, para enriquecerla y eliminar el estigma violento que se le pudiera atribuir. La resiliencia en el ámbito del Poder Nacional evoluciona, de hecho, el concepto de raíz.

El Poder Nacional está definido en el Glosario de Términos Unificados de la siguiente forma: "Capacidad de un Estado para alcanzar y/o preservar los Objetivos Nacionales. Se estructura con la

reunión de los recursos y medios de toda índole, disponibles y potenciales, organizados para su empleo estratégico. Para su análisis y estudio se puede dividir de manera convencional en los campos: político, económico, social, militar, tecnológico y diplomático" (p. 9).

Por ejemplo, siendo México una nación de naturaleza pacifista, es poco probable que utilice su poder nacional para imponer su voluntad a otros países y que hagan lo que se desea conforme a los intereses y objetivos nacionales. Si bien esta visión de poder nacional es posible, no se considera aplicable a México.

Cámez Meillón lo expresa de la siguiente manera: "[…] el problema es entonces la falta de una aproximación contemporánea de valor teórico del poder nacional, lo que posibilita una interpretación negativa (o agresiva) en su concepción y, en consecuencia, un rechazo por parte de países de política exterior pacifista y cooperativa, que evita la atención, sociabilización, aplicación y aprovechamiento de las virtudes del poder nacional" (p. 11).

Gran parte de la noción de una "imposición de voluntad" es de entenderse en países más desarrollados en los dominios del poder, como por ejemplo EUA, el hegemón del continente americano y posiblemente del mundo. Su naturaleza expansionista respalda esta visión (Rodríguez Sumano, 2018).

Basta con revisar la lista de autores que definen el poder nacional, muchos de extracción anglosajona o europea. Estudiosos del poder nacional en México como Vizarretea y Oliva, instituciones educativas como la UDLAP, Think Tanks como CASEDE, u organizaciones militares de las FFAA, programas de TV, reporteros y más podrían tener una visión distinta sobre el mismo término[2].

De esta forma, la defensa, poder nacional, junto con la seguridad y defensa nacionales tienen el objetivo final de contrarrestar amenazas que pongan en riesgo el bienestar y el desarrollo del país. La resiliencia se conjuga con ellos para lograr esta meta, pues si bien no es de carácter ofensivo, sí se requiere, en especial, cuando hay un incidente adverso. Esta idea la respalda de alguna manera Nye en su documento CiberPoder cuando indica que "la redundancia, la resi-

liencia y la respuesta rápida son componentes cruciales de la defensa (p. 5).

De hecho, un marco teórico sobre el poder nacional ampliamente utilizado en los últimos años es el que describe Joseph Nye (2004) en su libro *SoftPower. The Means to Success in World Politics*, en el cual delinea tres tipos de poder (ver Tabla 2), que posteriormente utiliza para ejemplificarlos en el ciberespacio (2010):

Tabla 2: Tipos de poder

Tipo	Característica	Reforzamiento	Ejemplos clásicos	Ejemplos en el ciberespacio
Duro (Hard)	Basado en recursos tangibles	Coerción	Producto interno bruto, equipamiento militar, etc.	Ataques de denegación de servicio y a infraestructura crítica
Suave (Soft)	Basado en recursos intangibles	Persuasión	Voluntad, cultura, normas y valores	Normas y estándares de ciberseguridad
Inteligente (Smart)	Basado en la combinación de los anteriores	Diplomacia	Elementos de defensa y desarrollo	No especificado por Nye

Elaboración propia basada en Cámez Meillón, 2020, considerando el ciberespacio.

Resulta interesante revisar cómo Cámez Meillón (p. 56) correlaciona esta clasificación del poder con los tipos de paz que describe Johan Galtung en sus obras, indicando por ejemplo que el poder duro se asocia con la paz negativa y el suave con la paz positiva, generando una paz imperfecta. En términos del ciberespacio, la que Cámez Meillón llama "paz imperfecta" sería una "paz tolerada", como el autor de este documento propone y que se explica en los siguientes párrafos.

Un punto importante a considerar en el marco de la Seguridad Nacional es el nivel de conflicto (paz-guerra) que se ha generado

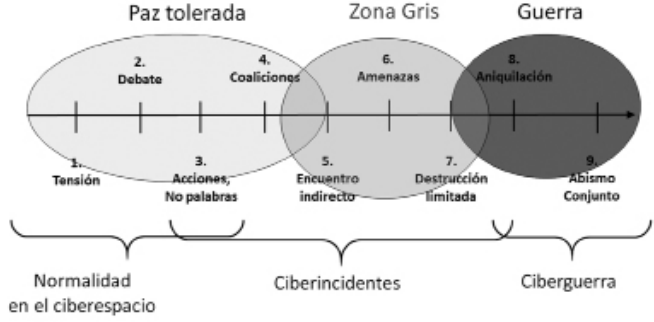
en el nuevo dominio de operaciones: el ciberespacio. El significado de "paz" es subjetivo y ha ido cambiando durante la historia del ser humano. A lo largo del tiempo se ha hablado de paz negativa, positiva, estructural, cultural, ambiental o engendrada (Oswald Spring, 2020:135), para poder identificar su acepción conforme a las circunstancias que se deseen expresar. Por ello, indiscutiblemente el término "paz" resulta ser polisémico y en continua evolución.

Así como el concepto de paz evoluciona, también lo hace el mundo tangible hacia el virtual, con el uso de la tecnología, y de la misma forma también se van incrementando los riesgos asociados (Ulrich, 1998).

Actualmente, en el entorno del ciberespacio, se podría hablar de una "paz tolerada", en virtud de que se presenta cuando los sistemas informáticos operan a pesar de estar bajo un escenario de riesgo continuo. Así pues, se tolera el riesgo, se acepta y se continúa operando.

No obstante, como se mencionó anteriormente, no ha existido una escalada en los conflictos en el ciberespacio que se torne en una declaración formal de guerra. Tomando en cuenta los incidentes registrados al momento, proponemos una ciberescalada de conflictos con base en la gráfica de Friedrich Glasl (1999), como se muestra en la figura 2:

Figura 2: Ciberescalada de conflictos



Elaboración propia basada en (Glasl, 1999) y (Votel, Cleveland, Connet y Irwin, 2016).

De esta forma, la paz tolerada que actualmente prima en el ciberespacio tiene una relación directa con la resiliencia en alguno de los niveles descritos en la tabla 2, la cual es un componente del "CiberPoder", término que se comentará en la siguiente sección.

Nuestra hipótesis es que no se podrá ser resiliente en los niveles de riesgo de la zona gris y guerra si no se alcanza la CR inteligente.

D. CIBERPODER

El ciberpoder (CP) es conceptualizado como la habilidad para utilizar el ciberespacio con fines de aprovecharlo e impactar en otros ambientes operacionales y a través de diversos campos del poder (Kramer, Starr y Wentz, 2009).

Por su parte, Nye, en su documento Cyberpower refiere este término indicando que "Cyberpower depends on the resources that characterize the domain of cyberspace" (p. 3) ("El ciberpoder depende de los recursos que caracterizan el dominio del ciberespacio") y lo define de la siguiente manera "Cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power" ("El ciberpoder es la capacidad de utilizar el ciberespacio para crear ventajas e influir en eventos en otros entornos operativos y a través de los instrumentos de poder").

De hecho, Nye (p. 5) indica cómo pueden aplicarse los tipos de ciberpoder conforme la clasificación de poder duro y suave para imponer la voluntad sobre otras naciones o influenciarlas a tomar determinada decisión:

- *Ciberpoder duro: Ataques directos tipo denegación de servicio, fugas de información sensible, modificación de comportamiento de sistemas de infraestructura crítica, etc.*
- *Ciberpoder suave: Imposición de normas, encarcelamiento de ciberdelincuentes, apoyo a activistas del ciberespacio (hacktivists) en contra de un gobierno, fakenews, warefare, espionaje, etc.*

No obstante, como se expuso anteriormente, Kramer y Nye son estudiosos del poder de origen estadounidense, por lo que su visión del ciberpoder es eminentemente de naturaleza ofensiva y no del todo aplicable a la CR, la cual "soporta" un incidente y busca evolucionar a la nación para mitigar los daños y mantener los objetivos nacionales.

Una definición propia de ciberpoder que complementaría las anteriores sería: "La capacidad de aprovechar la cuarta dimensión de operaciones (ciberespacio) en beneficio de otros campos del Poder Nacional, así como generar la capacidad para defenderse, soportar y recuperarse de ataques a los procesos que utilizan tecnologías de información, a fin de mantener la integridad, estabilidad y permanencia del Estado Mexicano".

En esta definición se puede observar que se emplea el ciberpoder también para recuperarse de ataques, término que está ausente en las definiciones de Kramer y de Nye.

Esta concepción amplía el espectro de aplicación del ciberpoder y evoluciona el término para adecuarlo a la situación actual. La CR sería la encargada de la recuperación hacia el nuevo equilibrio y, por tanto, es un componente integral del ciberpoder.

Siguiendo esta línea de pensamiento, la clasificación realizada por Nye de los tres tipos de poder podría utilizarse como punto de partida para definir los tipos de CP, como se muestra en la siguiente tabla, basada en las tablas 1 y 2.

Tabla 3: Aporte al Poder Nacional por parte del Ciberpoder			
Duro	Controles físicos de ciberseguridad	Planear/Preparar Absorber Recuperar	Equipos y medidas tecnológicas, edundancia, higiene tecnológica, monitorización
Suave	Controles administrativos de ciberseguridad		Políticas de seguridad, planes de recuperación y continuidad del negocio, simulacros y alianzas en su cadena de suministro
Inteligente	Controles psicosociales	Adaptar	Competencias del personal y características subjetivas de la organización
Elaboración propia			

De manera que el Ciberpoder total podría expresarse así:

- $CPT = xCPd + yCPs + zCPi$

Donde:

- *CPT = Poder total del CP*
- *CPd = Poder duro del CP*
- *CPs = Poder suave del CP*
- *CPi = Poder inteligente del CP*

x, y, z = Coeficiente de ponderación para el CP

Los coeficientes de ponderación (x, y, z) tienen gran relevancia en la expresión anterior, en tanto que ellos determinarán qué tan grande o pequeña es la contribución de cada tipo de CP en el CP total.

Aún más, una pregunta de investigación podría ser:

¿Cuál de esos elementos proporciona mayor ciber-resiliencia dentro del ciberpoder a lo largo del tiempo en que se desarrolla un ciberincidente, y que por tanto, contribuye en mayor medida al Poder Nacional?

Una hipótesis que manejamos es que la CR en el CP de corte inteligente es mucho más grande que las de tipo mayoritariamente duro y blando, esto es, que en términos de ciber-resiliencia los coeficientes x y y son mucho menores que z, por lo que al final la contribución de CPi es la que hace la diferencia para obtener una CR efectiva. O también porque son secuenciales en el sentido de que el CP suave depende o se determina en función del CP duro, y el inteligente depende de qué se tenga en las otras dos. Es decir, deben ser consistentes para ser efectivos. De nada sirve tener un plan de continuidad que supone una redundancia tecnológica si ésta no existe.

De hecho, los valores de los coeficientes de ponderación cambiarán conforme se avanza en el incidente. Por ejemplo:

- *Antes del ciberataque, el coeficiente x es más alto que y y z.*
- *Inmediatamente después del ciberataque, y es más alto que x y z.*
- *Conforme pasa el tiempo y se regresa a un estado operativo, z es el más importante y, por tanto, más grande que x y y. Éste es el punto donde entra de manera más clara la CR.*

Las competencias y características del CP inteligente serían, por ejemplo: flexibilidad, improvisación, liderazgo, comunicación efectiva, espontaneidad, intuición, colaboración, alianzas, etc.

Estos conceptos marcarían una diferencia fuerte entre una CR alta y una baja, siendo más importantes que los elementos del ciberpoder duro y suave en la CR cuando se desea regresar a la nueva normalidad, una vez que se ha pasado a la zona gris o a la de guerra, conforme al esquema de la Figura 2.

Como caso, un elemento como el liderazgo tendría un coeficiente bajo (p. ej. 1) en las etapas de Planear/Preparar y Absorber; un coeficiente medio (p. ej. 3) en la etapa de Recuperar; y un coeficiente alto (p. ej. 10) en la etapa de Adaptación.

Lo anterior también se confirma por lo que se ha visto en los incidentes que han ocurrido al momento en el entorno global, donde se reitera que no importa el estándar de ciberseguridad, controles avanzados, planes y protocolos aplicados: cualquier organización y una nación entera pueden ser víctimas de ciberataques avanzados.

La parte más importante en la resiliencia efectiva ocurre en el momento inmediato que sigue a la detección del incidente (un evento disruptivo que toma por sorpresa), pues se tiene que responder de manera oportuna, principalmente por seres humanos. Esto sin duda es independiente de la tecnología utilizada, es un tema eminentemente psicosocial.

Siguiendo esta línea de pensamiento, se puede decir que algunas de las técnicas de medición que se han seguido actualmente sólo toman en cuenta los elementos duros (p. ej. equipamiento de ciberseguridad) y los suaves (p. ej. protocolos de respuesta a incidentes), los cuales se considera que se traducen directamente en resiliencia.

Esto es un error: La ciberresiliencia en el CP inteligente puede hacer una gran diferencia entre seguir adelante o detenerse sobre todo en la fase adaptativa. En términos de seguridad nacional, sería la diferencia entre preservar los objetivos nacionales, degradarlos o perderlos.

Esta falla en la concepción del poder ha ocurrido con anterioridad. Muchas veces existen factores que no se habían tomado en cuenta y que son significativos en el poder que se ejerce. En este sentido, es de llamar la atención la forma en que el Centro de Política Pública evalúa el poder suave de las naciones (McClory, 2019).

Esta organización genera anualmente un índice que se basa en la clasificación de Nye, por lo que utiliza los tres pilares que de-

terminan el poder suave: valores políticos, cultura y política externa. Para conseguir el índice usa indicadores cuantitativos y cualitativos.

En el aspecto cuantitativo maneja 75 métricas de seis categorías principales mediante la obtención de datos estadísticos: cultura, educación, compromiso, perfil empresarial y gobierno. Para el aspecto cualitativo revisa siete categorías por medio de entrevistas: cocina, turismo, tecnología, productos de lujo, confianza, atracción y contribución a la sociedad global.

Uno de los indicadores de la cultura, por ejemplo, es el número de restaurantes con estrellas Michelin3. Cabría preguntarse por qué esto sería un indicador; la respuesta es simple: es un punto de atracción de visitantes que se captan y con un nivel económico que poseen. Pudiera no parecer una relación directa, pero ciertamente es una forma de ejercer el poder suave.

Esto indica claramente que no hay una sola forma de medir el poder suave: cada investigador puede seleccionar diferentes estadísticos, siempre y cuando influyan en el tipo de poder que representa. Por ello, se seleccionan algunos elementos no considerados abiertamente con anterioridad, como parte indispensable de un poder inteligente en la CR, como se señalan en este artículo.

Existen naciones, como México, que ostentan un ciberpoder bajo, sobre todo si solamente se considera el poder duro y suave; esto es, únicamente estándares de ciberseguridad, controles instalados, leyes u organizaciones (García Hernández, 2019), y no se han concretado aspectos como organizaciones dedicadas de tiempo completo a esta área, emisión de leyes focalizadas en ciberseguridad, materias sobre esto en educación básica, etc. Si esto lo traducimos directamente en la CR, se podría llegar a una conclusión errónea, indicando que la CR de este país también es baja.

E. CONCLUSIONES

Como ocurre en múltiples disciplinas, el entendimiento claro de los conceptos involucrados es de suma importancia para su comprensión y utilización correcta. Esto aplica a la seguridad nacio-

nal y al ciberespacio. El uso de términos del ciberespacio evoluciona el entendimiento y aplicación de los de seguridad nacional. Al final, resulta en una relación simbiótica en un círculo virtuoso que beneficiará ambos ámbitos, teniendo como triunfadores a los países que los saben entender.

Asimismo, su interpretación debe ser amplia y manejable en diversas situaciones. Por ejemplo, la definición del poder nacional bajo la óptica anglosajona no es la más afortunada para otros países, donde el poder también contiene otras características para la defensa nacional efectiva.

Como se señala anteriormente, algunos países con un bajo nivel de ciberpoder tradicional, con la visión descrita en este documento, pueden incrementar su poder en el ciberespacio, e incluso su poder nacional total. El resistir, adaptarse y evolucionar ante ciberataques podría convertirse en un gran aliado para recuperarse ante lo inevitable. La CR efectiva conlleva ese poder. La historia ha señalado en reiteradas ocasiones que no necesariamente sobrevive aquel organismo que tiene mayor fuerza, sino el que sabe evolucionar.

NOTAS

1. *Se ha dicho que podría haber sido Rusia, aunque aún no se cuenta con evidencia contundente al respecto.*
2. *Se sugiere dar seguimiento a las organizaciones y estudiosos señalados en (Heraldo de México, 2020).*
3. *Las estrellas Michelin son una referencia para determinar el nivel del restaurante por la experiencia culinaria que genera. Mayor información en https://guide.michelin.com/en. No obstante, si se toma en cuenta el poder inteligente del CP, el resultado podría cambiar radicalmente. Es posible que seguir normas y protocolos estrictos ocasione una falta de flexibilidad, lo cual disminuiría el CP total. Lo mismo ocurre si en CPi se consideran competencias como la espontaneidad e intuición, algo que en la cultura mexicana podría tenerse en mayor medida que en países sumamente disciplinados, cuya flexibilidad es menor e inexistente en la desviación de protocolos.*

RECONOCIMIENTOS

Se hace un reconocimiento de manera particular
al Dr. José de Jesús Vázquez Gómez (jjesusvg@banxico.org.mx)
por sus atentos comentarios sobre el contenido de este artículo.

REFERENCIAS

CÁMEZ MEILLÓN, S. (2020). *Sistema del poder nacional sostenible para México en el Siglo XXI.* CDMX, México.

CINTRA, J.T. (1991). *Seguridad nacional, poder nacional y desarrollo.* (S.d. Centro de Investigación y Seguridad Nacional, Ed.).

CISA (2020). *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (AA20-352A). Recuperado el 23 de diciembre de 2020 de https://us-cert.cisa.gov/ncas/alerts/aa20-352a

CSIS (2020). *Center for Strategic & International Studies.* Recuperado el 10 de octubre de 2020 de https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

DOMÍNGUEZ B., R y GARCÍA D., S. (2003). *Introducción a la Teoría del Conflicto en las Organizaciones.* Madrid, España: Imprime.

DUPONT, B. (2019). The Cyber-Resilience of Financial Institutions: Significance and Applicability. *Journal of Cybersecurity,* 1-17. DOI:10.1093/cybsec/tyz013

DUSSÁN H., O. (2005). Seguridad y Defensa Nacional (U.M. Granada, Ed.). *Prolegómenos. Derechos y Valores, VIII* (15), 104-122. Obtenido de http://www.redalyc.org/articulo.oa?id=87622620006

FIREEYE (2021). *M-Trends.* Obtenido de https://www.fireeye.com/current-threats/annual-threat- report/mtrends.html

GARCÍA H., A. (2019). *CiberMéxico: voluntades y acciones en el ciberespacio* (segunda edición). México: IUS Literatus.

GLASL, F. (1999). *Confronting Conflict. A First-Aid Kit for Handling Conflict.* Hawthorn Press.

GOBIERNO DE LA REPÚBLICA (2017). *ENCS. Estrategia Nacional de Ciberseguridad.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseg uridad.pdf

GOBIERNO EUA (2020). *USA GOV.* Recuperado el 8 de marzo de 2020 de https://www.usa.gov/espanol/como-funciona-el-gobierno

HALUANI, M. (2006). Orígenes históricos y componentes del poder nacional contemporáneo: factibilidad y utilidad de la medición empírica de las capacidades estatales. *Cuadernos del CENDES,* 23(61), 127-148.

HERALDO DE MÉXICO (28 de diciembre de 2020). *Lo mejor de la cultura de seguridad en 2020.* Recuperado el 3 de enero de 2021 de https://heraldodemexico.com.mx/opinion/2020/12/28/lo-mejor-de-la-cultura-de- seguridad-en-2020-239428.html

ITU (2020). *Global Cybersecurity Index.* Recuperado el 2 de enero de 2021 de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

KRAMER, F.; STARR, W y WENTZ (2009). *Cyberpower and National Security.* (N.D. University, Ed.). EUA: Potomac Books, Inc.

LSN (2005). *Ley de Seguridad Nacional.* México. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/ref/lsn.htm

McCLORY, J. (2019). *The SoftPower 30.* Portland. USC Center on Public Diplomacy. Obtenido de https://softpower30.com/what-is-soft-power/

NATIONAL ACADEMIES PRESS (2012). *Disaster Resilience. A National Imperative.* Washington DC, EUA.

NYE, J. S. (2004). *SoftPower. The Means to Success in World Politics.* N. York: Public Affairs.

_____ (2010). *CyberPower.* Harvard Kennedy School. Cambridge: President and Fellows of Harvard College.

_____ (2011). *The Future of Power.* EUA: Public Affairs.

_____ (2017). Deterrence and Dissuasion in Cyberspace. *International Security,* 41(3), 44- 71. DOI:10.1162/ISEC_a_00266

OSWALD S., Ú. (enero de 2020). Paz y seguridad engendradas, sustentables y culturalmente diversas. *Estudios de la Paz y Conflicto,* X(X), 116-142. DOI:10.5377/rlpc.v1i1.9519

OSWALD S., Ú. y GÜNTER B., H. (2009). *Reconceptualizar la seguridad en el siglo XXI.* Cuernavaca, México: Universidad Nacional Autónoma de México.

REAL ACADEMIA ESPAÑOLA (2020). *Real Academia Española.* Obtenido de https://www.rae.es/

RODRÍGUEZ S., A. (2018). *Granos de Arena* (1 ed.). México: Universidad Iberoamericana, A.C.

ROMERO G., J. (2018). Conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México. Universidad Autónoma de Tamaulipas, Ed. *Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM,* XXVIII (2). Recuperado el 2 de enero de 2021 de https://www.redalyc.org/comocitar.oa?id=65458498003

SEDENA-SEMAR (2018). *Glosario de términos unificados de seguridad nacional.* CDMX.

SINGER, P. y FRIEDMAN, A. (2014). *Cybersecurity and Cyberwar.* EUA: Oxford University Press.

SOTO S., J.E. (2009). La Defensa Nacional de la "A" a la "Z". Algunas definiciones y conceptos. (A.N. Estratégicos, Ed.) *Revista Política y Estrategia* (114), 291-317.

ULRICH, B. (1998). *La Sociedad del Riesgo.* Barcelona, España: Paidós.

VOTEL, J.; CLEVELAND, C.; CONNET, C. y IRWIN, W. (enero de 2016). Unconventional Warfare in the Gray Zone. *Joint Force Quarterly*, 101-109.

ARTURO GARCÍA HERNÁNDEZ

Funcionario del Banco de México, doctorante del posgrado en Defensa y Seguridad Nacional de la Universidad Naval. Maestro en Seguridad Nacional por dicha institución educativa y Maestro en Ciencias en Sistemas Distribuidos por la Universidad de Kent en Inglaterra. Estudioso de la ciberseguridad y sus aplicaciones prácticas para el Estado Mexicano. Líneas de investigación: defensa y seguridad nacional, ciberseguridad, infraestructuras críticas.

Correo E.: arturo.garcia.hdez@gmail.com