ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

100/2014 12 septiembre de 2014

*José María Molina Mateos**

GLOBALIZACIÓN, CIBERESPACIO Y ESTRATEGIA
ESPECIAL CONSIDERACIÓN A LA ESTRATEGIA DE LA INFORMACIÓN

GLOBALIZACIÓN, CIBERESPACIO Y ESTRATEGIA
ESPECIAL CONSIDERACIÓN A LA ESTRATEGIA DE LA INFORMACIÓN

Resumen:

El proceso globalizador en el que estamos inmersos, derivado del descomunal desarrollo de las comunicaciones y el impacto de las finanzas ha configurado una mutación de la sociedad mundial en todos los órdenes que abre en el nuevo espacio relacional surgido de la misma un horizonte de oportunidades y riesgos sin precedentes en la historia. La magnitud y complejidad del ciberespacio, ámbito paradigmático de esta nueva realidad, auténtica "sobrenaturaleza" artificial de carácter electrónico, demanda una estrategia internacional para su plena consolidación y desarrollo, como forma de arraigar y hacer viable un entorno en el que sea posible el progreso de la humanidad con plena garantía de intereses, derechos y libertades, en un marco de paz y seguridad internacional. Y que dada su naturaleza informacional requiere de forma especial y como premisa, el desarrollo de una estrategia de la información inspirada en los valores y principios derivados de los textos internacionales sobre Derechos Humanos y los valores del Estado de Derecho, atendiendo a las posibilidades que brindan las tecnologías más avanzadas.

Abstract:

The globalization process in which we are immersed, derived from massive development of communications and the impact of finance has set a mutation of world society in all areas open in the new relational space emerged from it, a horizon of opportunities and risks unprecedented in history. The magnitude and complexity of cyberspace, paradigmatic scope of this new reality, true artificial "Supernatural" electronic in nature, demand an international strategy for full consolidation and development as a way to consolidate and make possible an environment where possible progress of humanity with full guarantee of interests, rights and freedoms, within a framework of international peace and security. And given their informational nature requires special shape and premise, the development of an information strategy inspired by the values and principles derived from international instruments on human rights and the values of the rule of law, based on the possibilities offered by the most advanced technologies.

Palabras clave:

Ciberespacio, la ciberseguridad, globalidad, internacional, estrategia, digital, seguridad, seguridad de la información, la tecnología y la seguridad de las comunicaciones, las libertades públicas en el ciberespacio, la seguridad internacional, la seguridad global, la seguridad cibernética global.

Keywords:

Cyberspace, cybersecurity, globality, international, strategy, digital, security, information security, technology and communication security, public freedoms in cyberspace, international security, global security, global cybersecurity.

José María Molina Mateos

"Hoy el hombre no vive ya en la naturaleza sino que está alojado en la sobrenaturaleza que ha creado en un nuevo día del Génesis: la técnica."
(Ortega y Gasset)

INTRODUCCIÓN

Las necesidades derivadas de los requerimientos, amenazas, retos y oportunidades procedentes de la utilización del ciberespacio ejercen una fuerte presión bajo la forma de demanda intelectual y de pensamiento que, de no ser atendida, corremos el riesgo de ser desbordados por los acontecimientos. Llegando a ser el ciberespacio uno de los sectores más necesitados de materia gris del planeta y la causa del mayor consumo del apreciado combustible neuronal.

En estas circunstancias, el pensamiento estratégico español tiene ante sí la tarea de profundizar y seguir la evolución y desarrollo de la Estrategia Nacional de Seguridad 2013 y la Estrategia Nacional de Ciberseguridad derivada, aprobadas durante el pasado año, mediante las que el Gobierno de España implanta de forma coherente y estructurada las acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas. Y, además atender a las exigencias generales de carácter global, conformadoras del marco de actuación en el que nos encontramos inmersos. Ambas tareas vienen a ser complementarias.

En el escenario que se abre a consecuencia de la digitalización de la sociedad mundial, esta doble circunstancia invita a reflexionar desde una triple perspectiva -global, regional y local- y permite contribuir con la comunidad internacional para la consecución de una paz y seguridad, justa, estable y duradera.

Como señala Göra Therborn[1], en las diferentes olas históricas de la humanidad, siempre ha estado presente la tendencia globalizante, entendida como la aceleración o intensificación de grandes procesos sociales de alcance e impacto, al menos, de nivel continental.

Según Osterhammel y Peterson[2], ha sido precisamente, la última de estas olas las que ha dado su nombre a la "globalización" en la expresión y alcance conceptual que ha tenido a

[1] Recogido por Göran Therborn en su obra "The World: A Beginner´s Guide".
[2] Globalization, a short history, Princeton University Press, 2005.

partir de finales de la década de los ochenta. El tiempo implosionó en el espacio y el futuro ha pasado a ser un extenso ámbito globalizado, dominado por la espacialidad.

La globalización es una fuerza supraindividual en la que las conexiones y el impacto se expanden sin dirección ni sentido concreto y es representativa de la mezcla de un cambio rápido con una paralización transformadora.

Tras los acontecimientos de 1989-1991 todo pasó a ser global de la mano de los nuevos medios de comunicación electrónicos que permitieron conectar el planeta a gran velocidad. La sensación predominante de esta ola, sin precedentes en la historia, fue su carácter único. Su manifestación más tangible fue la extensión de los mercados, la apertura de los movimientos de capital y el comercio de mercancías y servicios, lo que produjo como consecuencia ineludible una competencia global. En su dimensión social, la globalización ha supuesto un aumento de la conectividad planetaria y la migración cultural.

La globalización ha sido guiada por dos corrientes principales, una constituida por el descomunal desarrollo de las comunicaciones y la revolución que ha supuesto (fundamentalmente Internet como medio de comunicación global, la televisión por satélite y los canales digitales) y otra la financiera.

Al menos en términos comerciales y financieros, el significado de la ola de la globalización parece que anuncia un cambio a partir de la crisis que comenzamos a abandonar, dejando de ser solo una extensión de los mercados y redes virtuales y de la compresión espacio temporal para ser, además, la confirmación del cambio del centro de gravedad económico y político de Occidente hacia el mundo asiático.

Los canales electrónicos están cambiando el juego de la política sin que se conozca hasta dónde llegará. De momento sus efectos aperturistas parece que han superado los obstáculos expresados a través de nuevas formas de vigilancia y control –a reservas de determinar las consecuencias que todavía pudieran tener los hechos puestos de manifiesto en el caso Snowden– que no han desvirtuado hasta hoy el probable efecto de la globalización y la hiperconectividad.

Están por ver los efectos en la globalización que produzca la corriente securitaria, muy especialmente, en su dimensión informacional, y si los puntuales episodios de "renacionalización" cibernética, generalmente vinculados a intentos antidemocráticos de control político interno, no dejan de ser una mera anécdota, contraria a la lógica y a la política de los tiempos o, por el contrario, conforman una efectiva aparición de fronteras electrónicas, con lo que ello supondría de freno al proceso globalizador. Sin olvidar que junto

a este proceso se ponen de relieve a diario otros de signo opuesto, de diferenciación simbólica y naturaleza antropológica, que se manifiestan bajo la forma de tribalización, particularismo étnico o procesos análogos. El resultado es el punto crítico de equilibrio entre esta tendencia globalizadora supranacional y la reducción del ámbito para el ejercicio de la acción política que, al día de hoy, se sigue encarnando en el Estado-nación.

Con la finalidad de tratar de comprender la corriente de la globalización, constituida por la revolución de las comunicaciones y su producto más característico representado por el ciberespacio y los riesgos que se derivan de su uso, se aborda una aproximación al fenómeno desde una perspectiva amplia, centrados en este ámbito y su seguridad –la ciberseguridad– convencidos de que es la mejor forma de abordar la dimensión estratégica del fenómeno digital y su relación con la seguridad internacional.

Partiendo de una delimitación conceptual del sistema ciberespacial y el subsistema cibersecuritario, se hace especial énfasis en la necesidad de neutralización de las ciberamenazas que deriva en un análisis de la ciberseguridad desde perspectivas distintas, de forma que transciende los tradicionales enfoques de seguridad vinculados a las dimensiones militares o tecnológicas del problema, para situarse en una nueva categoría que requiere otras dimensiones para su eficacia, como son la económica, la política, la organizacional o la jurídica.

El ciberespacio es una realidad compleja, con múltiples dimensiones, que demanda una profunda reflexión sobre el mismo para, de este modo, ir elaborando un pensamiento que contribuya a la configuración del armazón intelectual necesario, capaz de crear las categorías precisas, que esté a la altura de su importancia y riesgos consiguientes, desde el que articular una ordenación y seguridad eficientes que permitan la protección real y efectiva de intereses, derechos y libertades.

La ciberseguridad es una realidad que surge para neutralizar las amenazas derivadas de la utilización del ciberespacio, que requiere soluciones concordantes con su configuración y con los problemas que estas plantean, en una diversidad de juegos relacionales que dan lugar al complejo conflicto cibersecuritario, cuya solución se aborda a través de la técnica del balanceo ponderado de los distintos intereses en juego.

En el momento actual del estadio de la ciberseguridad, se ha considerado necesario hacer una aproximación a la misma desde una perspectiva general y, en cierto modo, que contribuya a la necesaria toma de conciencia de un fenómeno que resulta de alto interés para la Sociedad, el Estado, las corporaciones, las empresas y los individuos, a nivel global, por ser el ciberespacio una realidad que envuelve irremisiblemente la vida actual y de cuya

utilización se derivan enormes oportunidades de todo tipo, pero también nuevos riesgos que exigen ser neutralizados.

Las ya significativas, aunque aún insuficientes, iniciativas locales expresadas a través de estrategias nacionales se orientan en la buena dirección de proporcionar una respuesta de los estados a los problemas de seguridad en el ciberespacio desde la perspectiva de países concretos.

Las no menos significativas, pero también insuficientes, respuestas regionales, refuerzan las anteriores, confirman la bondad del camino emprendido y ponen de relieve la necesidad de dar el paso a una iniciativa de este género, de ámbito internacional.[3] Lo que lejos de ser el hito inmediato siguiente, en la secuencia lógica de ámbitos, supone un salto cualitativo considerable por la complejidad que comporta la necesidad de dar respuesta a una multitud de intereses en juego, derivados de culturas y sistemas políticos y jurídicos diferentes, con desarrollos tecnológicos disímiles, cuyo tratamiento requiere de una mínima armonización para que pueda tener éxito.

La comprensión del fenómeno es una cuestión de capacidades intelectivas, conocimiento y razón, pero también de actitud ante la complejidad como representación más característica de los actuales momentos en los que continúan chirriando los goznes de la historia a consecuencia del cambio de era.

La asimilación de las consecuencias políticas, económicas, sociales y culturales, en todo caso, se ha de hacer desde la perspectiva de los principios y valores democráticos. (Aunque, se da la circunstancia que según el estudio de 167 países por la Unidad de Inteligencia de The Economist, 166 son estados soberanos y 165 son miembros de Naciones Unidas, 25 son democracias plenas, 54 son democracias imperfectas, 37 son regímenes híbridos y 51 son regímenes autoritarios, y ello podría desalentar el buen fin). Sin embargo, el reconocimiento de varios de los principios y valores básicos que afectan a la ciberseguridad ya están recogidos en los textos internacionales sobre Derechos Humanos y, al menos formalmente, en las constituciones de todos los países del globo.

Respecto a la tecnología, ya el ilustre filósofo y pensador Ortega y Gasset, dijo en 1933 que *"…lo que nadie puede dudar es que desde hace mucho tiempo la técnica se ha insertado entre las condiciones ineludibles de la vida humana de suerte tal que el hombre actual no podría, aunque quisiera, vivir sin ella. Es pues, hoy una de las máximas dimensiones de nuestra vida, uno de los mayores ingredientes que integran nuestro destino…".* Por tanto,

[3] Un intento unilateral en esta dirección es la International Strategy for Cyberspace, de mayo de 2011, aprobada por el Presidente de los Estados Unidos, cuyo contenido puede ser indicativo.

respecto a la tecnología se podrán hacer muchas afirmaciones, excepto la de que no forma parte consustancial de la vida humana, así ha sido y así seguirá siéndolo en el futuro.

Habida cuenta que la tecnología es el elemento físico básico, configurador del ciberespacio, el acceso y conocimiento a la misma ha de estar, de aquí en adelante, al alcance de todos los ciudadanos del mundo como un derecho esencial para la convivencia humana en la nueva sociedad en la que estamos inmersos.

En la combinación de las dimensiones de la ciberseguridad y la necesaria colaboración entre actores, se ha de destacar el protagonismo alcanzado por la respuesta legal, que configura la dimensión jurídica como uno de los soportes de la ciberseguridad y recomienda dedicarle un estudio específico.

ESTRATEGIA

Tras el final de la Guerra Fría el concepto de estrategia parece haber cedido en la atención de los investigadores para centrarse en el de seguridad cuya definición ha de implicar a toda la comunidad, la preservación de sus valores esenciales, ausencia de amenazas y la formulación de objetivos políticos, su tema son los actores estatales y no estatales (organizaciones no gubernamentales y organizaciones intergubernamentales, entre otros).

La estrategia es definida en el Diccionario de la Lengua Española[4] y en el *Webstger´s Third New International Dictionary*[5]. Veinticinco siglos después de *Sun Tzu* y un siglo después de *Klausewitz*, la estrategia ha ampliado su espectro y es una ciencia incipiente en el ámbito empresarial. Tiende a ser prescriptiva, normativa, a convertirse en algo administrativo, predecible, cuantificable y controlable.

La estrategia tiene una lógica paradójica, es un fenómeno objetivo en el cual las condiciones surgen, las quieran o no sus participantes, se den cuenta o no de sus alcances. En la estrategia las circunstancias se juntan, se pueden volver en contra, hoy pueden ser favorables pero mañana pueden haberse convertido en amenazas. Lo que maneja la estrategia son discontinuidades potenciales que podrían plantear amenazas o presentar oportunidades.

[4] "1. Arte de dirigir las operaciones militares. 2. Arte, traza para dirigir un asunto. 3. En un proceso regulable, el conjunto de las reglas que aseguran una decisión óptima en cada momento".
[5] "la ciencia y el arte de emplear las fuerzas políticas, económicas, psicológicas y militares de una nación o de un grupo de naciones para darle el máximo soporte a las políticas adoptadas en tiempos de paz o de guerra".

Quienes gestionan los destinos de un país, han de hacer lo mismo, sumergirse e interactuar en sus realidades nacionales e internacionales y crear un punto de vista respecto al futuro.
El pensamiento estratégico anterior a la era nuclear se ocupaba de cómo combatir y ganar.
Los modernos estudios estratégicos hunden sus raíces en el siglo XIX, hasta la Segunda Guerra Mundial, periodo en el que las corrientes de pensamiento se orientaban hacia el aumento de la dimensión y la rapidez de la guerra, en relación con el tamaño de las sociedades que las generaban, así como el parecido –cada vez menor– de una nueva guerra, con las que la precedieron. Todo ello, en base al *aumento de riqueza y mayor organización de las naciones y la innovación tecnológica*.

Las guerras adquirieron tales dimensiones, que el coste de la guerra era mayor que el beneficio de la victoria.

El impacto del conflicto ocasionado por las reflexiones sobre la Gran Guerra (1914-1918), abrió una brecha física y psicológica entre dos épocas.

En el periodo de entreguerras se sigue pensando en la guerra, aunque los más creativos esperaban restablecer la eficacia de los métodos militares y ponían sus esperanzas en las nuevas tecnologías. Tras la Segunda Guerra Mundial –y sobre todo, tras el lanzamiento de las bombas atómicas sobre Hiroshima y Nagasaki –quedó muy claro que la guerra total se había convertido en un instrumento irracional de las relaciones entre las superpotencias. En este esquema de pensamiento, resultaba inconcebible un objetivo nacional que justificase el coste de involucrarse en un conflicto de semejante magnitud, como no fuese el último: la supervivencia.

La nueva situación estratégica creada, fue definida por *Bernard Brodie* en 1.946, con la siguiente frase: "*Hasta ahora el fin del estamento militar era ganar guerras, de ahora en adelante será evitarlas. Casi no existe otro fin útil*".

A partir de este momento se produce un cambio sustancial en el pensamiento estratégico y emerge la defensa como concepto central e, indudablemente, con el arma atómica en el escenario de una disuasión contenida durante años.

La presencia y permanencia del arma atómica, así como los intentos de proliferación, y posteriormente, el terrorismo internacional y las armas de destrucción masiva, introducen una dimensión particularizada en los estudios estratégicos que, entendemos, no afecta a la aproximación genérica que se pretende.

Con la caída del Muro de Berlín en 1.989 y el final de la Guerra Fría, se da un nuevo paso en el pensamiento estratégico. Se percibe con claridad, que la recíproca dependencia de los Estados en la vida internacional, lleva a la necesidad de abordar cualquier eventual solución de ámbito nacional desde una perspectiva global.

Existen una serie de realidades mundiales que determinan la prosperidad, los logros sociales o las libertades públicas de cada país. Las soluciones a estos problemas se podrán materializar en la medida que las grandes decisiones que configuran la vida nacional se adapten, con precisión, a una exacta percepción de lo que es el ambiente internacional.
El nivel de vida de los ciudadanos, su poder adquisitivo, la consistencia de sus instituciones, son consecuencias de acciones internas, pero enmarcadas en los enfrentamientos económico-mundiales en los que participan todos los países y cuyo resultado es el equilibrio global.

En este juego global internacional cada nación persigue de una forma prioritaria la consolidación de su seguridad como meta tradicional de su política exterior.

El concepto de seguridad nacional[6], hoy, rebasa ampliamente su componente militar para ser producto de una delicada combinación de factores políticos, ecológicos, diplomáticos, tecnológicos, sociales o culturales.

El modo de vida de los ciudadanos, sus intereses, la consistencia de sus instituciones, la defensa de sus libertades, su seguridad, se sitúan en el punto de intersección entre los grandes ejes de la política nacional con las variables de una nueva configuración mundial.

Hoy, la seguridad de cada país y la paz mundial están amenazadas por peligros económicos, tecnológicos, sociales e institucionales en similar medida que por peligros militares.

La pérdida de soberanía económica de un país, o la dependencia tecnológica, pueden suponer el debilitamiento, e incluso la extinción de su autonomía política, con una subordinación de las libertades y el nivel de vida, de sus ciudadanos a poderes exteriores a los que no se podría controlar.

Actualmente aparecen otras amenazas ligadas al escenario internacional tales como la pobreza, la degradación del medio ambiente, las migraciones humanas, el terrorismo, el

[6] "La acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos" (España, Estrategia de Seguridad Nacional 2013).

crimen organizado, las amenazas cibernéticas, las armas de destrucción masiva, la droga o las pandemias, que constituyen fenómenos trasnacionales que no conocen fronteras y vienen a comprometer gravemente la supervivencia de toda nación económica y militarmente soberana.

Con todo ello, se pueden apreciar unos claros nexos de unión entre política exterior, economía, tecnología, ecología o política interior.

El ciudadano, debe conocer que sus derechos individuales, sus libertades, su seguridad en definitiva, se juegan en una partida mundial cuyo resultado depende de todos.
El concepto de estrategia ha ido evolucionando y, en cada una de las situaciones descritas, tenía una dimensión y un alcance distinto.

La importancia de la estrategia radica, entre otras cosas, en la selección del esfuerzo político y militar en un escenario, de tal forma que logre una síntesis que permita resolver las cuestiones presentes, con clara visión de los escenarios futuros resultantes de las mismas.
Lo que demanda un esfuerzo conjunto y multidisciplinar, caracterizado por la complejidad de elementos interrelacionados y por la incertidumbre de una amenaza no convencional, transnacional y sin respeto al Derecho Internacional.[7]

Con todo lo indicado, y a modo de una síntesis intensificada, se podría intentar efectuar una aproximación al significado del concepto de estrategia en el momento actual, en el que, algunos autores la identifican con el concepto de “Política” (con mayúscula).

Como destilado resultante del conjunto de factores intervinientes, la estrategia podría configurarse como la adaptación de recursos, medios y capacidades de la Nación, al entorno cambiante en el que esta se desenvuelve, con directa repercusión en el aprovechamiento de oportunidades y evaluación de riesgos, en función de unos objetivos marcados por el Gobierno.

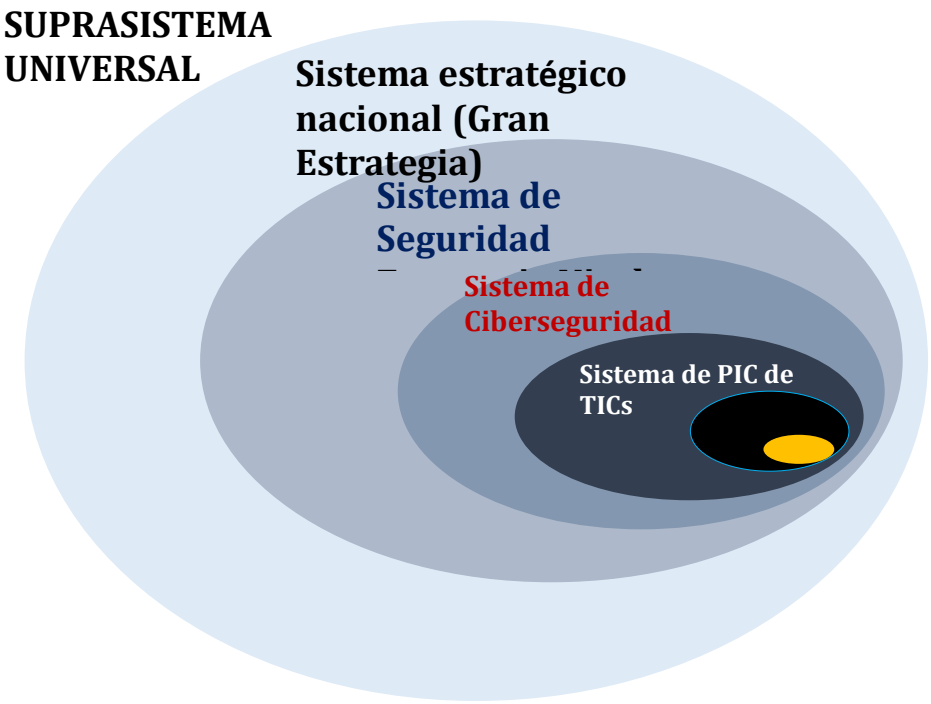
Este concepto se corresponde con el de *Estrategia General de la Nación*, o *Gran Estrategia* (que pocas naciones tienen y de la que tal vez sería conveniente disponer) que, desde una perspectiva de país, sería lo que se conoce como *estrategia de primer nivel*.

Dentro de la Nación, cada uno de los elementos más significativos de su vida activa, tienen a su vez una estrategia, que responde al mismo concepto, pero de forma sectorial, así se puede hablar de estrategia económica, estrategia política, estrategia de seguridad…, entre otras, y constituirían lo que se conoce como estrategias de segundo nivel.

[7] “Para bellum: la estrategia de la paz y de la guerra”, Edward N. Luttwak, Edit. Siglo, Madrid, 2005.

De igual modo y dentro de los ámbitos de las estrategias de segundo nivel, los elementos más significativos pueden tener a su vez una estrategia, que responde al mismo concepto indicado, pero referido a un ámbito más reducido aún que el sectorial, como sería, por ejemplo, dentro de la seguridad, la estrategia militar, la estrategia policial, la estrategia de inteligencia o la estrategia de ciberseguridad, que serían estrategias de tercer nivel[8].

En un cuarto nivel se situarían las estrategias que dentro de los ámbitos del tercer nivel fuesen necesarias para la articulación de sus elementos más significativos. Si tomamos como ejemplo la estrategia de ciberseguridad, cabría la posibilidad de hablar de estrategias relativas a sus ámbitos predominantes como son la "seguridad de los equipos", "seguridad de las redes", "seguridad de los sistemas", "seguridad de la información" y "protección de infraestructuras críticas de las TICs."



(Fuente: Autor)

La jerarquización de estrategias en un ámbito indicado, conlleva la necesaria subordinación de las estrategias a los ordinales anteriores lo que se traduce en que han de estar configuradas en coherencia con los mismos y no pueden estar en oposición a ellos. Lo que

[8] En España, al no existir una Estrategia General o Gran Estrategia de país, por lo que la jerarquización de los niveles comienzan en el ámbito siguiente, y la estrategia de ciberseguridad es una estrategia de segundo nivel, como indica la Estrategia Española de Seguridad en su último párrafo.

en términos sistémicos supone que han de actuar en el sentido de actuación marcado desde el ente de nivel superior.

Dicho esto, nada impide –y generalmente es así– que un ámbito de orden subordinado pueda, en otro orden de cosas, ocupar un nivel diferente.

Entre los desafíos de la seguridad están algunos, tributarios del pasado y otros más modernos, que suponen una ampliación del concepto, supera la oposición entre seguridad militar y seguridad civil que, a través de una visión ampliada, incluye nuevos actores y nuevas dimensiones no militares.

Las fronteras entre la seguridad militar y política está fragmentada, lo que, en cierto modo, sería indicador de que el Estado ya no tiene capacidad para resolver en solitario los problemas de seguridad. Son continuas las referencias a la seguridad regional, internacional e incluso, global que ha dado lugar a conceptos como el de seguridad cooperativa o seguridad común, lo que supone una colaboración entre actores estatales y no estatales como fórmula para resolver los conflictos de seguridad.

Esta sería la situación de la ciberseguridad que requiere el desarrollo de capacidades militares y civiles para la defensa y explotación de los sistemas de información, tanto a nivel nacional como comunitario (en el caso europeo) y con socios y aliados para asegurar que un país pueda defenderse de los ataques cibernéticos y pueda tomar medidas contra los adversarios allá donde se encuentren. Para conseguirlo, ha de recurrir a los métodos clásicos de cooperación entre Estados y abrirse a una colaboración internacional aún mayor.

ESTRATEGIA INTERNACIONAL

El carácter global y alta complejidad del ciberespacio requiere de una estrategia internacional para su utilización y desarrollo que armonice los distintos componentes que entran en juego.

Esta necesidad se pone de relieve en la iniciativa de Barak Obama, Presidente de los Estados Unidos, mediante la Estrategia Internacional para el ciberespacio de mayo de 2011,[9] que aun habiendo sido elaborada unilateralmente desde un Estado-nación, puede servir como modelo de referencia para otra que, eventualmente, se realice de forma multilateral bajo los auspicios de Naciones Unidas.

[9] International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World, May 2011, President of the United States.

Esta iniciativa viene a justificar la realización de un enfoque estratégico partiendo de los éxitos obtenidos, reconociendo los desafíos a los que se enfrentan las sociedades y garantizando la preservación de los principios fundamentales al hacerlos frente.

Para ello declara el compromiso del mantenimiento y mejora de los beneficios derivados de las redes digitales para las economías y sociedades.

Parte del reconocimiento de que el crecimiento de estas redes trae consigo nuevos desafíos para la seguridad nacional, la económica y la de la comunidad global, a los que se hará frente preservando los principios fundamentales, las libertades, la privacidad y el libre flujo de información.

Hace una declaración del futuro del ciberespacio estableciendo unos objetivos generales y fijando otros para la diplomacia, la defensa y el desarrollo.

Como objetivo general la estrategia señala que se trabajará a nivel internacional para promover una información abierta, interoperable, segura y confiable, por la infraestructura de comunicaciones que soporta el comercio internacional, fortalece la seguridad y fomenta la libertad de expresión e innovación. Para ello se propone la construcción y mantenimiento de un entorno de normas de comportamiento responsable que guíe las acciones de los estados, así como celebrar acuerdos de colaboración y apoyo al Estado de Derecho en el ciberespacio.

Se propone una estabilidad a través de las normas incidiendo en su papel y fundamentos de forma que esté plenamente garantizada la defensa de las libertades fundamentales, el respeto a la propiedad, la valoración de la privacidad, la protección contra el delito, el derecho de autodefensa, la interoperabilidad global, la estabilidad de la red, una accesibilidad fiable, participación de las múltiples partes interesadas del gobierno y debida diligencia en la ciberseguridad. Fija un nuevo papel para el ciberespacio futuro basado en las tres “D”: *diplomacia, defensa y desarrollo*.

Como *objetivo diplomático* se fija trabajar con el fin de crear incentivos para construir un consenso internacional en el que los estados reconozcan el valor intrínseco del ciberespacio en una sociedad abierta, interoperable, segura y confiable, en el que trabajen juntos y actúen como partes interesadas responsables, mediante el fortalecimiento de las asociaciones bilaterales y multilaterales, organizaciones internacionales y de múltiples interesados y colaboración del sector privado.

Como *objetivo de la defensa* señala la disuasión y la prevención, con fuerzas en el interior y en el exterior. Se fomentará el comportamiento responsable y se opondrán a quienes tratan de interrumpir las redes y sistemas, a fin de disuadir a los agentes maliciosos, reservándose el derecho de defensa de estos bienes nacionales e internacionales, vitales, como sea necesario y apropiado.

Como *objetivo del desarrollo* se fija la prosperidad y la seguridad. Naciones Unidad facilitará la creación de capacidades de ciberseguridad a fin de que cada país disponga de los medios para proteger su infraestructura digital, fortalecer las redes globales y construir en consenso una asociación más estrecha de redes seguras y confiables con normas abiertas y compatibles, mediante la creación de capacidades técnicas, capacidades de seguridad y construcción de relaciones políticas.

La estrategia fija una serie de prioridades políticas basadas en la economía, la protección de las redes, la aplicación de la ley, la defensa militar, la gobernanza de Internet, el desarrollo internacional y la libertad de Internet.

En el plano económico promoverá normas internacionales, comercialización de productos innovadores y mercados abiertos, para lo que se mantendrá un entorno de libre comercio que fomente la innovación tecnológica y redes de acceso relacionadas a nivel mundial, protegerá la propiedad intelectual incluyendo los secretos comerciales e industriales y garantizará la primacía de las normas técnicas interoperables y seguras, determinadas por expertos técnicos.

En lo referido a la protección de las redes propias, se mejorarán la seguridad, fiabilidad y resistencia, para lo que promoverá la cooperación en el ciberespacio, en particular en las normas de comportamiento para los estados y la seguridad cibernética, bilateralmente y en una amplia gama de organizaciones y asociaciones multilaterales. Asimismo se reducirán las intrusiones en las redes y las interrupciones, se garantizará una gestión robusta de incidentes, resistencia y capacidad de recuperación de las infraestructuras de información y se mejorará de acuerdo con la industria, la seguridad de la cadena de suministros de alta tecnología.

En la aplicación de la ley se ampliará la colaboración y el Estado de Derecho mediante la participación en el pleno desarrollo de políticas internacionales sobre delitos cibernéticos; armonización de leyes internacionales sobre el cibercrímen mediante la ampliación de la adhesión a la Convención de Budapest; dando un enfoque a las leyes sobre delitos informáticos para que combatan las actividades ilegales sin restringir el acceso a Internet y

negar a los terroristas y otros criminales la posibilidad de aprovechar Internet para sus ataques y la planificación técnica, operativa y financiera.

En el plano militar se propone preparar los desafíos para la seguridad del siglo XXI, mediante el reconocimiento y adaptación a la creciente necesidad de redes militares fiables y seguras; construcción y mejora de alianzas militares para hacer frente a posibles amenazas en el ciberespacio, y ampliar la cooperación ciberespacial con aliados y socios para aumentar la seguridad colectiva.

Respecto a la gobernanza de Internet, promoverá estructuras eficaces e inclusivas, priorizando la apertura y la innovación en Internet, preservando la seguridad de la red y la estabilidad mundiales, incluidos los sistemas de nombres de dominio y mediante la promoción y mejora de las partes interesadas locales para la discusión de las cuestiones de gobernanza de Internet.

En lo relativo al desarrollo internacional se creará capacidad, seguridad y prosperidad, proporcionando los conocimientos necesarios, la capacitación y otros recursos para los países que buscan fortalecer la capacidad técnica y la ciberseguridad. Se desarrollarán continua y regularmente y se compartirán las mejores prácticas internacionales de seguridad cibernética, se mejorará la capacidad de los estados para combatir la ciberdelincuencia, incluida la formación de la policía, médicos forenses, juristas y legisladores, y se desarrollarán relaciones con los políticos para mejorar la capacidad técnica, proporcionando un contacto regular y permanente con los expertos. Respecto a la libertad en Internet se apoyará a las libertades fundamentales y la privacidad, mediante el apoyo a los actores de la sociedad civil en el logro de las plataformas fiables y seguras, y de las libertades de expresión y asociación. Colaborará con la sociedad civil y organizaciones no gubernamentales para establecer garantías de protección de su actividad en Internet de intrusiones digitales ilegales, se fomentará la cooperación internacional para la eficacia de la protección de la privacidad de los datos comerciales y garantizará la interoperabilidad de extremo a extremo de un Internet accesible para todos.

Naciones Unidas efectuará una llamada al sector privado, la sociedad civil y usuarios finales, así como invitará a los estados y pueblos a unirse en la realización de esta visión de prosperidad, seguridad y apertura en un mundo interconectado.

En este espacio resulta de especial importancia su seguridad. La ciberseguridad[10] ha sido definida por la OCDE como *la propiedad del ciberespacio consistente en la capacidad de resistir a las amenazas intencionales y no intencionales, responder a ellas y recuperarse*.

CONSIDERACIÓN ESPECIAL SOBRE LA ESTRATEGIA DE LA INFORMACIÓN

Para realizar una aproximación a la estrategia de la información se requiere singularmente y de forma previa, identificar las funciones básicas a realizar respecto a la información para, sobre ellas y sus relaciones con las demás, establecer un posicionamiento estratégico, inspirador de todo cuanto se derive o tenga relación con las mismas.

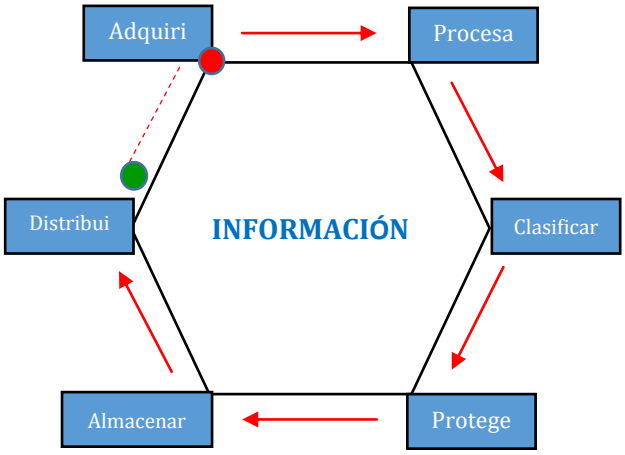
El proceso se irá enriqueciendo mediante el añadido de los componentes de cada una hasta elaborar un sólido cuerpo estratégico, depurado y aceptado por todos.

Para poder avanzar, se requiere tener un concepto claro y compartido de lo que es "información", lo que es "estrategia" y los principios que han de inspirar una "política de información".

Considerando que todo lo relacionado con la información está impregnado de política, antes de abordar una estrategia de información, se ha de determinar los principios que han de inspirar una política de información en una moderna sociedad democrática, partiendo de la base que el secreto, *per se*, debilita la democracia, pero es necesario para el mantenimiento de la misma, en concretos y precisos asuntos, y en ocasiones contadas, la privacidad es condición indispensable de los derechos ciudadanos y que la transparencia inspira y anima la convivencia social sana y democrática.

Al objeto de este trabajo, se pueden identificar seis funciones básicas de la información que para su mejor visualización las situaríamos en los vértices de un hexágono regular: adquirir, procesar, clasificar, proteger, almacenar y distribuir.

[10] O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. "Ciberseguridad: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan".



Adquisición

La adquisición de información se puede realizar por los procedimientos más diversos que van desde la producción propia a su obtención mediante compra, a través de los medios de comunicación, por conducto de los canales diplomáticos, de los servicios de información e inteligencia, la procedente de la investigación y la ciencia, de la cultura en general o de otras fuentes.

Una estrategia de adquisición sistemática sería aquella que relacionase todas estas fuentes y determinase de cuales se dispone o no, cuales son las preferentes, o cuales requieren de una implantación, potenciación o perfeccionamiento.

Entre los procedimientos de adquisición de información habría que destacar por su importancia las actividades propias de los servicios de información e inteligencia y la fuga positiva o negativa de cerebros, hecho de forma estratégica y organizada, altamente significativa por cuanto se deriva del poder que disponen algunos científicos y cerebros más capacitados.

La percepción de la importancia de la adquisición de información, como base del conocimiento, permite albergar que, en un futuro se le dé similar importancia que a las adquisiciones físicas. Cuando eso llegue, será cuando se habrá llegado realmente a la sociedad del conocimiento con todo lo que ello comportará en la valoración económica y jurídica, no solo política, de los activos del mismo.

Procesamiento

El procesamiento de información, consiste en recibirla, elaborarla y actuar de acuerdo con ella. Actualmente en esta función interviene de forma determinante las TICs.

El componente de los sistemas tecnológicos que realiza esta tarea recibe la denominación de procesador, cuya función principal es la coordinación de los diferentes elementos del equipo. Ejecuta las aplicaciones, procesa sus instrucciones y da respuesta a las órdenes que envía a través de los periféricos de entrada. Lo que realiza mediante la combinación de hardware de silicio, o tecnología que en el futuro la sustituya, y el conjunto de componentes lógicos para la realización de su tarea específica, constituido por el software, producto estrella del procesamiento.

Clasificación

La información es de naturaleza e importancia muy diversa y cualquier estrategia requiere distinguir con nitidez, mediante *clasificación*, los bloques esenciales de los que se derivan tratamientos diferentes entre los que destacan la información pública y la privada. Dentro de cada uno de estos bloques, los subgrupos diferentes en virtud de la naturaleza específica y la asignación de niveles en función de la transparencia o sigilo que requieran.

Para la clasificación se requiere atender a los elementos esenciales configuradores de una política de información para los que se pueden tomar como referencia los derivados de los tratados internacionales sobre derechos humanos y los textos constitucionales de todos los países del globo[11], donde la práctica totalidad recoge –al menos en la letra–, de una u otra forma, los principios y excepciones que resumidamente se indican a continuación y que, en el caso español se plasman en los artículos 18.3 y 20 de la Constitución:

- **Transparencia de lo público y secreto de lo privado, como norma general.**
- **Secreto de lo público y transparencia de lo privado, como excepción.**
- **Un secreto público muy intenso, pero poco extenso.**
- **Un secreto privado, muy extenso y tan intenso como permita la real y efectiva aplicación del ordenamiento jurídico.**

Toda estrategia de información requiere inexorablemente incluir su defensa y ser consciente de que esta exigencia es proporcional a la cantidad de información manejada debido a su

[11] https://www.constituteproject.org/#/

gran fragilidad y falta de linealidad, de donde se deriva que pequeñas aportaciones, puedan tener consecuencias desproporcionadas.

Para satisfacer las necesidades de la protección se ha desarrollado la seguridad de la información que se extiende a la tecnología que hace posible su tratamiento y comunicación, estimulando una profunda y constante investigación y desarrollo, de productos, sistemas y aplicaciones criptológicas, que permiten lograr una efectiva integridad, accesibilidad, autenticación y confidencialidad de la información protegida. Lo que está permitiendo hacer planteamientos respecto a la universalización del cifrado, con lo que ello supone para la transparencia, que requiere de una fina regulación impregnada de alta sensibilidad política para solucionar las colisiones que se producen entre distintos derechos en conflicto.

¿Cuál es la seguridad necesaria para alcanzar la libertad posible en el mundo digital?
Con independencia del orden en que se formule la pregunta, articular una respuesta requiere profundizar en los instrumentos políticos, jurídicos y tecnológicos que hacen posible su respuesta pero, sobre todo, demanda adentrarse en la información, elemento cognitivo y racional, de naturaleza inmaterial, en torno al cual se han articulado las tecnologías que configuran el ciberespacio: las TICs.

Las tecnologías no dejan de ser herramientas para conseguir un fin predeterminado, por tanto, tienen la única responsabilidad de ser efectivas en el logro de los objetivos para los que han sido concebidas y solo, en base a esta capacidad de cumplir eficazmente con su cometido, cabe la posibilidad de evaluarlas. El objetivo no debe santificar ni demonizar las tecnologías utilizadas para conseguirlo, pues estas tienen un carácter medial aunque, en el plano jurídico tenga consecuencias que pudieran ser diferentes, dada la necesidad de su "cooperación" para la realización de determinados hechos.

Será por tanto el fin, el objetivo que se pretende conseguir, lo que ha de ser merecedor del calificativo correspondiente. Pero ese fin, generalmente, suele ser solo una parte de un todo más complejo.

Una tecnología puede ser buena o mala protegiendo información o procesándola, almacenándola, comunicándola, etc. Al final, se puede apreciar que todo este conjunto de fines y objetivos son distintos aspectos relacionados con un elemento de entidad autónoma con respecto al cual actúan: la información.

El almacenamiento

La acumulación de información para poder disponer de ella en momentos posteriores configura lo que se conoce como almacenamiento e implica la conservación y posibilidad de recuperación, así como requiere orden, facilidad de acceso y garantía de perdurar en el tiempo, sin merma de los distintos elementos que la configuran.

La función de almacenamiento de la información siempre ha sido conceptual y fácticamente esencial, pero ha ido adquiriendo cada vez mayor importancia debido la explosión informacional ocurrida con la llegada de las TIC´s y a la voracidad despertada en su consumo.

Distribución

Aunque la información se haya adquirido, procesado, clasificado, e incluso, protegido, de poco sirve si no se pone en disposición de su destinatario en el momento oportuno. De ahí la necesidad abordar la distribución como un factor de naturaleza estratégica, que incrementa su complejidad cuando se trata de hacer planteamientos de carácter internacionales y más aún, si tuviese un carácter global.

Una política de distribución implica la indicación de quien tiene acceso a qué tipo de información así como los medios para llevarlo a cabo, y está en intima conexión con la clasificación, la protección y el almacenamiento.

Para la distribución resulta esencial la infraestructura de comunicaciones con todo lo que implica en cuanto a tecnología, interoperabilidad y seguridad, con sus políticas, estrategias, planes y medios específicos.

CONCLUSIÓN

Como quiera que las TICs son el elemento físico que hace posible el ciberespacio y que la información es el objetivo y finalidad al servicio de los cuales estas actúan, la información resulta ser un elemento determinante para configurar la libertad y la seguridad en el ciberespacio, por lo que una estrategia sobre la misma parece ser el punto de partida para la construcción de un ciberespacio equilibrado, libre, seguro y pacífico. En consecuencia con todo lo anterior, se puede considerar que elaborar una estrategia de información es la premisa imprescindible para, sobre ella, construir el modelo que ciberespacio que se quiere. Y ello desde una perspectiva sistémica, en la que estaría integrado tanto el nivel internacional representado por Naciones Unidas, que marcaría la dirección del conjunto, como los entes regionales y los gobiernos de los Estados e, incluso, dentro de estos, las administraciones públicas y las entidades privadas empresariales o profesionales.

Todo ello configuraría un gran sistema estratégico de la información que sería el *"core"* y punto de partida en el que se asentarían las bases de otros sistemas estratégicos (como el tecnológico o el jurídico, informacional, jurídico-informacional, o jurídico-informacional-securitario), que integran el ciberespacio, así como las estrategias que se elaboren sobre este, que constituiría el gran paso definitivo en la progresión de formular un concepto sistemático y último de la información del que derivarían los demás.

Naciones Unidas está tomando iniciativas para tratar de alcanzar un consenso general y establecer una normativa internacional que promueva el acceso universal a las tecnologías de la información y las comunicaciones, al tiempo que garantiza la seguridad en la Red y la protección de la información. Y, en su seno, España dispone de una gran oportunidad, en el bienio 2014-2015, para hacer valer internacionalmente sus posiciones como miembro del Grupo de Expertos Gubernamentales sobre Ciberseguridad, en virtud de la resolución 68/243 de la Asamblea General.

Se podría considerar que esta deseable normativa requiere previamente de un consenso político sobre las variables esenciales —críticas al estar relacionadas con la información— que se plasme en una estrategia internacional sobre el ciberespacio que incorpore un ajustado diagnóstico del ciberdilema y todas sus aristas, e incluya estrategias internacionales de segundo nivel sobre la información, la tecnología y el derecho, cuyo resultado sería la base para la elaboración de una estrategia global de ciberseguridad, punto de referencia y fuente de inspiración de la normativa que la desarrolle, en base a la que poder caminar con éxito hacia la paz digital.

[i]

*José María Molina Mateos**
Doctor en Derecho
Máster Universitario en Estudios sobre Paz, Seguridad y Defensa
Especialista en Criptología
Profesor visitante de la Universidad Camilo José Cela
www.molinamateos.com