ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

17/2012 21 febrero de 2012

*Ángel Gómez de Ágreda**

EL CIBERESPACIO COMO ENTORNO SOCIAL Y DE CONFLICTO

# EL CIBERESPACIO COMO ENTORNO SOCIAL Y DE CONFLICTO

## Resumen:

Entre el 24 y el 27 de enero tuvo lugar en Londres el Sexto Seminario de Ciberdefensa y Seguridad de Redes[1]. Buena parte de los asuntos tratados en este trabajo formaron parte de las discusiones que tuvieron lugar allí. El Ciberespacio ha revolucionado la forma de vivir y de organizase en las últimas décadas. Su ritmo de evolución no ha dejado de crecer. De forma paralela a las posibilidades que ofrece, se han incrementado también los riesgos y amenazas que supone. Pero el entorno cibernético es, no obstante, mucho más que un escenario de conflicto, es un nuevo hábitat para la parte de la Humanidad que vive en el Mundo Conectado.

*Abstract:*

*The Sixth Cyberdefence and Network Security Seminar took place in London from the 24th to 27th of January. Most of the topics dealt with in this work were also discussed during the Seminar. Cyberspace has revolutionized the way we live and organize ourselves during the last few decades. Its evolutionary rhythm has not ceased to increase. Parallel to the chances it offers, risks and threats have grown too. But the cyber domain is, nonetheless, much more that the scenery of a conflict, it is a new habitat for the part of Mankind who lives in the Connected World.*

## Palabras clave:

Ciberespacio, redes, informática, comunicaciones, orgánica, defensa, seguridad, internet.

*Keywords:*

*Cyberspace, networks, informatics, communications, organization, defence, security, internet.*

[1] http://www.cdans.org/Event.aspx?id=598092

*"El Ciberespacio es el conjunto de un dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones"*[2].

Esta definición es tan buena como otras muchas que hay del nuevo espacio conformado por la combinación de la capacidad de computación de la informática y la de transmisión de datos de las nuevas tecnologías de comunicaciones. Igual que la mayoría de ellas, sin embargo, peca de un exceso de peso tecnológico en su planteamiento. Nos cuenta de forma clara y concreta en qué consiste el espacio cibernético y enumera sus posibles usos, pero se queda muy lejos de introducirnos en las implicaciones que tiene su mera existencia.

El Ciberespacio es mucho más que el conjunto de máquinas que nos permiten la explotación del espectro electromagnético para comunicarnos; incluso más que la información que se mueve por él. Lo que hemos construido va incluso más allá de un nuevo espacio de confrontación donde es posible hacer más y mejores negocios, legales e ilegales. En el espacio virtual estamos forjando nuevas personalidades, nuevas identidades y nuevas formas de relación que replican –como si fuera un universo paralelo –las actividades que llevamos a cabo en el mundo físico.

No entender que las relaciones que establecemos a través de las redes sociales son tan reales como las de "barra de bar" equivale a pensar que los pagos con tarjeta de crédito nos van a costar menos que sus equivalentes en dinero contante y sonante. El Ciberespacio no es equivalente a los ámbitos terrestre, naval, aéreo y espacial como muchos afirman, es una réplica de un mundo físico completo en la cual siguen existiendo las mismas necesidades y vulnerabilidades pero donde las reglas de funcionamiento son básicamente distintas. Las redes sociales no son un entretenimiento de adolescentes, sino una nueva forma de socializar y de entender el mundo donde el grupo deja de ser determinante en la personalidad de sus miembros para que éstos pasen a construir tantos grupos como intereses distintos tengan.

Martin C. Libicki[3] dividía el Ciberespacio en las tres capas clásicas: la física, que está formada por el *hardware* de todo tipo que empleamos para albergar e interactuar con la información; la semántica, constituida por esos mismos datos; y la sintáctica, que está conformada por los programas y protocolos que nos permiten gestionar estos últimos.

[2] Dan Kuehl, "Cyberspace & Cyberpower: Defining the Problem", *Cyberpower & National Security*, 2009.
[3] Ph.D. in economics, M.A. in city and regional planning, University of California, Berkeley; S.B. in mathematics, Massachusetts Institute of Technology

Con frecuencia olvidamos que las tres son fuente de vulnerabilidades de importancia equivalente que deben ser atendidas correspondientemente. Tendemos a ver el *hardware* como aquello que tenemos al alcance de la mano y que accionamos directamente: el ratón, la CPU, la impresora, el monitor,… incluso, en el mejor de los casos, los cables y enrutadores que nos conectan con el exterior de nuestro hogar u oficina. Sin embargo, como en otros ámbitos, hay cosas más grandes y más pequeñas que las que tenemos a la vista y que también forman parte del mundo y suponen vulnerabilidades.

No tenemos ningún –o escaso –control sobre los cables submarinos que conforman nuestras redes de datos, ni sobre los servidores que albergan los datos que manejamos en "la nube", ese concepto que alude al almacenamiento remoto de información y programas. Tampoco prestamos, en multitud de ocasiones, suficiente atención a los detalles pequeños. Los componentes individuales en que se divide nuestro equipo ofrecen, cada uno de ellos, sus propias puertas de acceso, peligros y posibilidades. En ninguno de esos casos solemos tener el menor control sobre el proceso de su fabricación o sobre su gestión.

Ponemos, eso sí, mucha más atención en la fortaleza de nuestro sistema en lo que se refiere a la capa sintáctica y a la semántica. Protegemos nuestros equipos con antivirus y cortafuegos e invertimos tiempo y dedicación en la generación de complicados sistemas de acceso restringido en un esfuerzo asimétrico que no tiene en cuenta el principio de que toda cadena se rompe por el eslabón más débil.

La proliferación de dispositivos móviles que aprovechan la tecnología inalámbrica para llevar la información al último rincón y que tanto nos facilitan nuestro trabajo y nuestro ocio diario, añade una nueva brecha a la muralla de nuestra seguridad informática. No nos engañemos, esos pequeños dispositivos con los que recibimos nuestro correo electrónico mientras vamos en el Metro o en el autobús forman parte del Ciberespacio tanto como los potentes ordenadores que utilizan las empresas o la Administración. Las vulnerabilidades que se introduzcan a través de ellos en un sistema pueden ser tan peligrosas como cualquier otra y el hecho de que no exista conexión física entre los terminales, no supone protección alguna.

Sin embargo, los ataques procedentes de *hackers* aficionados en busca de notoriedad, emociones o diversión, y que son la causa principal de preocupación para la mayor parte de la población, apenas si siguen teniendo lugar. El amateurismo ha desaparecido prácticamente del Ciberespacio para dar paso a la profesionalización de las intrusiones. Cuando una vulnerabilidad descubierta en un programa o proceso se paga en el mercado negro a decenas de miles de dólares, o puede proporcionar beneficios a su explotador de cantidades aún mayores, queda poco sitio para la mera gamberrada casual. Internet se ha

poblado de organizaciones especializadas en cada uno de los escalones del delito informático, desde el descubrimiento de las vulnerabilidades hasta el blanqueo de los fondos obtenidos con su explotación, pasando por la utilización de redes de miles de ordenadores para la comisión de delitos o de denegaciones de servicio equivalentes a la destrucción temporal de los equipos.

Las agresiones que tienen lugar en la actualidad proceden de este tipo de grupos o de Estados nacionales que emplean el Ciberespacio como un entorno más en el que llevar a cabo una "competencia sin restricciones" en todos los terrenos: económico, financiero, diplomático, comercial, militar,… La guerra en el siglo XXI se ha sustituido por un continuo tensar la cuerda de las relaciones procurando obtener el mayor beneficio del desequilibrio del adversario.

Por eso, cuando hablamos de las vulnerabilidades de la capa física tenemos que hacer referencia a hechos como el desvío de tráfico de datos a servidores asiáticos durante dieciocho minutos en 2010 y que constituyó una prueba de la capacidad de los Estados para acceder a los datos que circulan por la red y, potencialmente, apropiárselos. No podemos olvidarnos de otros como la seguridad de los cables submarinos y, muy en particular, de los nodos principales, ni de la vulnerabilidad que supone la inclusión de procesadores y otros componentes de procedencia no controlada en nuestros equipos. La fabricación de componentes en terceros países es una puerta abierta a la inclusión de códigos maliciosos en los mismos que permitan la apertura de accesos a nuestros sistemas sin tener siquiera necesidad de contactar con nuestros equipos. En este sentido, el desarrollo de una industria capaz de llevar a cabo las investigaciones y el desarrollo de tecnologías punteras y de proveer a nuestro propio mercado de los componentes necesarios sería la opción más deseable. De no ser viable esta posibilidad, nuestros expertos deberán ser capaces de certificar la limpieza de los componentes instalados en aquellos equipos que vayan a formar parte de nuestras redes más sensibles.

Es precisamente en la capa humana, que falta en el esquema de Livicki, donde reside la mayor amenaza para la seguridad de nuestras redes. "No hay parches para la estupidez humana". La frase se ha convertido ya en un clásico; sobre todo después de la constatación empírica que supuso la filtración que dio origen a la publicación en la página de *Wikileaks* de cientos de miles de documentos que habían sido extraídos de una red interna por un usuario autorizado, un *insider*.

Si hacía falta alguna prueba de que los muros que nos proporcionen seguridad tienen que elevarse a un nivel similar en todo el perímetro, esta fuga de información puso de relieve la necesidad de una política informativa adecuada respecto de los riesgos que acechan en el

Ciberespacio que llegue a todos los usuarios, sea cual sea su nivel de acceso. Nada parece indicar que la adopción de medidas en función de su mayor o menor atractivo o visibilidad, en lugar de un estudio sistemático de los riesgos a afrontar, vaya a dar mejores resultados en el entorno cibernético que la pobre protección que proporciona en el mundo físico.

Se ha hablado y escrito mucho sobre los riesgos de intrusión en nuestros sistemas informáticos. El espionaje y el robo de datos y de identidades se ven facilitados por el alcance universal que obtienen los atacantes y la falta de concienciación sobre los riesgos del público general. Sin duda, ésta es la actividad más frecuente de las que tienen lugar en la actualidad. Hasta el punto que la obtención de información e inteligencia en la red, de meramente económica, ha pasado a convertirse en un arma política; como lo demuestran los recientes ataques mutuos entre *hackers* saudíes e israelíes en los que el robo de datos sobre tarjetas de crédito particulares adoptaba justificaciones e intencionalidad política en el contexto del conflicto árabe-israelí[4].

No obstante, esa visión de las acciones en el Ciberespacio no es reconocida universalmente. Siendo bastante representativa de la visión occidental y china de las operaciones en el espectro electromagnético, es radicalmente distinta de la aproximación que hace la Federación Rusa en su doctrina[5]. Para Moscú, el espectro electromagnético es una forma más de acercarse al control de la información para la configuración de las percepciones y la difusión de narrativas. Esta visión del Ciberespacio quedó evidenciada durante las operaciones en la guerra ruso-georgiana de 2008 en la que los efectos de los ataques de denegación de servicio distribuidos se sintieron más en la moral de la población y en su capacidad de resistencia y confianza en sus instituciones que en el campo operacional. Mucho más que la influencia en las redes de Mando y Control o que los problemas de índole económica y financiera causados, fue el aislamiento y la sensación de impotencia lo que influyó más negativamente en la voluntad de lucha de los georgianos.

Visiones tan distintas del papel del Ciberespacio entre distintos Estados y sensibilidades tan diferentes entre las distintas generaciones convierten en una labor extremadamente difícil el hecho de llegar a un acuerdo sobre unas normas de comportamiento cívico para el espacio virtual equivalentes a las que rigen nuestra convivencia física. Lejano el objetivo de conseguir unos acuerdos internacionales equivalentes a los convenios que rigen los conflictos o, por poner un caso más cercano, la Convención de las Naciones Unidas sobre la

[4] Se trata de iniciativas de particulares que comenzaron con un ataque de un *hacker* saudí que se hizo con los datos de miles de tarjetas de crédito de ciudadanos israelíes y los distribuyó con el único fin de perjudicar al "enemigo sionista". De forma paralela, ataques organizados por el grupo *Anonymous* han dejado sin servicio a varios organismos oficiales israelíes como protesta por la política de asentamientos en los territorios ocupados.
[5] "Visión conceptual de la actividad de las Fuerzas Armadas de la Federación Rusa en el espacio de la información", www.mil.ru

Ley del Mar, será necesario fijar, cuanto menos, un código de conducta que evite que internet se convierta en un entorno inhabitable[6].

La velocidad a que se producen los acontecimientos en la red hace que las agresiones suelan tener mayor probabilidad de éxito que las defensas. Esto es cierto tanto respecto de las acciones delictivas que pretenden el lucro económico como de las operaciones con un carácter más o menos bélico. Tan acusada es la diferencia a favor de los ataques que las estrategias del Ciberespacio no contemplan la posibilidad de establecer un sistema a prueba de cualquier intento de intrusión. Es por ello que se ha desarrollado el concepto de *resiliencia*, que designa la capacidad de recuperar la operatividad después de un ataque, habiendo minimizado los daños sufridos. En un caso ideal, el rebote, la recuperación, supone al mismo tiempo una adaptación a la nueva amenaza y una suerte de inmunización frente a la misma[7]; un rebote hacia adelante, hacia una posición más ventajosa.

El Ciberespacio requiere la gestión del riesgo más que la ilusión de su erradicación. Como ha quedado demostrado en numerosas ocasiones, no hay un sistema que sea totalmente hermético y a prueba de intrusiones, por lo que deberemos ser capaces de escalonar las medidas en función de la necesidad de protección de cada recurso. La posibilidad de que un ataque cibernético resulte incapacitante[8] nos obliga también a elaborar planes de contingencia que soslayen la utilización de los medios habituales sin dañar gravemente la eficacia de la organización.

Llegamos así a la conclusión de que las defensas en el Ciberespacio deben basarse, además de en los medios tecnológicos, en la formación del personal usuario de base y en su concienciación de que los riesgos asumidos por él se transfieren a la organización en su conjunto. Por otro lado, equipos especializados deben de ser capaces de establecer una estrategia pro-activa frente a las agresiones y de realizar análisis forenses de las amenazas para determinar su naturaleza y origen. Esta aproximación dual de información/formación de base y equipos de expertos no es, sin embargo, una labor que pueda ni deba ser asumida de forma aislada por la Administración, la empresa y la academia sino que tiene que resultar

[6] El 23 de noviembre de 2001 se estableció el "Convenio del Consejo de Europa sobre Cibercriminalidad" que, ni por extensión geográfica, ni por alcance temático se aproxima siquiera a lo que es necesario.

[7] Por esta razón, propuse la traducción de *resilience* como "resistencia adaptativa" en "*Globalización y resistencia adaptativa*", Boletín de Información del CESEDEN número 316, pág. 77-79, año 2010.

[8] La teoría de la "primera batalla" plantea la falta de profundidad estratégica del Ciberespacio, donde no existen "frentes" definidos y donde los ataques pueden alcanzar hasta lo más recóndito de nuestro sistema. Según dicha teoría, esta falta de profundidad supone que un primer ataque puede resultar completamente incapacitante y dejar al enemigo sin modo de reacción (al menos por medios cibernéticos, y muy debilitado en cuanto a su capacidad para gestionar cualquier otro). Esta circunstancia, unida a la superioridad de los ataques respecto de las defensas, convierten al Ciberespacio en un entorno donde estas últimas tienen que ser pro-activas en lugar de reactivas; en previsión de que no exista esa posibilidad de reacción.

de la convergencia de esfuerzos de los tres ámbitos y generar un paraguas común. Es necesaria una aproximación global del Estado, que incluya a actores públicos y privados, en lo que se viene llamando "aproximación del conjunto del Estado" (*whole of State approach*).

Probablemente, la solución venga de la mano de un paquete modular adaptable a las necesidades de cada uno y que comparta en su concepción los conocimientos y los requisitos de todos los usuarios finales. La imposición de unos ciertos niveles de protección en determinados entornos privados debe ser una responsabilidad del Estado en tanto que dichos servicios tienen un carácter crítico para la prestación de los que aquel está obligado a proporcionar.

El Reino Unido ha creado una Unidad de especialistas dentro de sus Fuerzas Armadas basada en una mezcla de personal en activo y personal reservista. El personal no fijo de la estructura, los reservistas, permite escalar las operaciones en función de las circunstancias, a la vez que incorpora los últimos conocimientos de la industria y permite interactuar con ella. Al mismo tiempo, la íntima relación entre unos y otros componentes habilita la posibilidad de una mejor comprensión de las necesidades de ambos e, incluso, del mismo lenguaje en que se hablan, muchas veces incomprensible para los profanos en la otra materia.

Este conocimiento y concienciación debe basarse, no en una mera información teórica de las amenazas y oportunidades que presenta el Ciberespacio, sino en una convivencia con las mismas. La inclusión de las operaciones cibernéticas en los ejercicios habituales de nuestras Fuerzas Armadas y de nuestra Administración en general son la mejor manera de conseguir este objetivo. Las guerras de los próximos años no tendrán lugar, con toda probabilidad, exclusivamente en el espectro electromagnético, pero resulta inimaginable que éste no esté presente en todas y cada una de ellas en mayor o menor medida.

También serán necesarios ejercicios específicos para el entrenamiento de las Unidades especializadas en la defensa de las redes propias. Como se apuntaba más arriba, las agresiones en el Ciberespacio, además de producirse en combinación con otras de otros tipos, tienen lugar con carácter continuo. Todos los días se producen miles de ataques a las webs corporativas de las distintas administraciones, y no se debe circunscribir la defensa de las mismas a los momentos de tensión o crisis sino que debe hacerse de forma continuada e ininterrumpida. Son necesarias soluciones imaginativas. En este sentido, el personal necesario para dotar a las unidades especializadas debe tener un carácter muy distinto al clásico del soldado de línea. El pensamiento innovador y crítico, la capacidad de anticipación, la curiosidad y el aventurismo deben formar parte de su bagaje para poder hacer frente a los hackers rivales.

Una buena dosis de esta mentalidad se requerirá también de los legisladores que tienen – más temprano que tarde – que hacer frente a los retos que supone crear un cuerpo normativo adaptado a los tiempos. Si el Ciberespacio se ha convertido en un hábitat más para el hombre, el establecimiento de las normas que regulen la convivencia en el mismo será tan necesario como en cualquier otro de ellos. Podemos hacernos eco de las palabras del Vicepresidente de los Estados Unidos en el sentido de que "los principios de Derecho Internacional no están suspendidos en el Ciberespacio" pero también tenemos que ser realistas y no olvidar que las características de este nuevo entorno requieren de una visión mucho más ágil y dinámica que la sociedad está reclamando.

Los ataques que se produjeron durante el año pasado a algunas instancias gubernamentales francesas motivaron al Presidente de la República, el Sr. Sarkozy, a convocar a los directivos de las principales empresas relacionadas con el Ciberespacio para estudiar el modo en que se puede regular su utilización. El rechazo frontal de muchos de ellos – y de buena parte de la sociedad – a una simple extensión de las normas y convenciones existentes al nuevo entorno quedó patente en el frío recibimiento que recibieron sus invitaciones y, posteriormente, sus propuestas mismas.

Para empezar, cualquier legislación sobre estos temas deberá contar con un amplio grado de consenso internacional que permita su aplicación sin tener en consideración las fronteras de los Estados nacionales existentes. La universalidad del acceso a la información y la fragmentación de los nodos para el mismo implica la necesidad de que las decisiones que se tomen tengan en cuenta a todos – o, al menos, a un número significativo de – los países, ya que, en la mayor parte de los casos, las acciones que tienen lugar en el Ciberespacio no se ven afectadas por limitaciones a las que sí están sometidas las jurisdicciones estatales.

Es cierto, como demostró el caso de Egipto en los primeros momentos de las revueltas que desembocaron en la caída del Presidente Mubarak, que se puede limitar y casi cercenar completamente el acceso a las redes en un país completo forzando a las compañías que operan las señales a discontinuar su actividad. Sin embargo, a las pocas horas de producirse el cierre, algunos grupos ya estaban conectados de nuevo a nodos internacionales a través de líneas telefónicas convencionales y al ingenio de unos pocos. Establecido el modo de conexión, la misma estructura reticular y la mentalidad de los "nativos digitales", hacen que sea muy sencilla la expansión del número de sus usuarios.

Quizás por esa razón dijo el Premier británico, Cameron, en la Conferencia sobre el Ciberespacio de Londres, que siguió al Seminario sobre Ciberdefensa y Seguridad de Redes de los días 24 a 27 de este mes de enero, que "no podemos avanzar por la vía de la mano dura. Si lo hacemos, destruiremos todo lo que de bueno tiene internet", para añadir más

tarde que "los Gobiernos no pueden utilizar la Ciberseguridad como excusa para la censura (…) Internet no pertenece a los Gobiernos, los Gobiernos no dan forma a internet". Aunque la red de redes nació de una iniciativa gubernamental, su desarrollo vino de la mano de la libertad y de la falta de prejuicios, de la confianza y de la voluntad de compartir conocimientos. Internet se impregnó de un cierto espíritu "hippie" que le permitió crecer con la rapidez y diversidad que lo ha hecho durante estas pocas décadas desde su nacimiento. La seguridad nunca fue una prioridad para sus diseñadores ni sus desarrolladores. Cuando estaba circunscrito al ámbito del Pentágono, su reducido alcance y difusión y la misma seguridad que proporcionaba la habilitación de sus usuarios, la convertía en prácticamente redundante. No serían muchos los que se plantearan la necesidad de añadir una protección adicional a un sistema cerrado y tan novedoso. Cuando, posteriormente, se abrió al mundo y se "civilizó", las ventajas que proporcionaba su carácter libre superaban, con mucho, a los inconvenientes que podían suponer los esporádicos ataques que sufrían los sistemas de entonces.

Internet es mucho más que un entorno en el que trabajar, convivir o pelear. Lleva asociada una orgánica propia, una estructura en la que los terminales son, de forma simultánea, nodos de la red que transmiten y retransmiten los datos que les llegan. Esta relación no es solamente técnica sino que termina siendo cultural y determina la capacidad de una organización o de un individuo para aprovechar las ventajas y oportunidades que presenta el Ciberespacio. Las viejas organizaciones verticales de estructura piramidal se adaptan mal al dinamismo y flexibilidad que requiere su uso y explotación; y, sin una capacidad notable para explotar los recursos que nos ofrece la red, no es posible competir en el mundo actual.

El uso de aplicaciones informáticas en la gestión de procesos y en su operación remota ha abierto la posibilidad de la utilización del Ciberespacio como medio transmisor de ataques dirigidos contra las infraestructuras así controladas. Los sistemas SCADA (*System Control And Data Acquisition*) de control de sistemas y adquisición de datos se encargan de la operación de centrales eléctricas, plantas nucleares, sistemas de comunicaciones y otros procesos que, por su complejidad y necesidad de precisión, requieren de una monitorización constante. El empleo del virus Stuxnet contra las centrifugadoras que se encargan del enriquecimiento del uranio en Irán puede considerarse un gran éxito desde el punto de vista de la utilización de medios cibernéticos para conseguir un fin. Los técnicos calculan que el retraso que supuso en la puesta en marcha del programa nuclear iraní puede cifrarse en un año y medio; probablemente, más de lo que hubiera conseguido un ataque aéreo contra las mismas instalaciones.

Stuxnet plantea, no obstante, dos dilemas. En primer lugar, demuestra una vez más la dificultad para realizar una atribución (de responsabilidades) fundamentada de los ataques

informáticos. Es prácticamente imposible determinar, en tiempo útil, la autoría de un ataque bien perpetrado; por lo que es igualmente difícil justificar una respuesta a dicho ataque, incluso si se emplean, como dice la doctrina americana y pretenden hacer los británicos, medios no necesariamente informáticos para llevarla a cabo. En segundo lugar, el empleo de armas cibernéticas capaces de actuar fuera del ámbito del Ciberespacio abre la puerta a que alteraciones de su código den lugar a herramientas similares que puedan ser empleadas contra nuestras propias infraestructuras. Otros virus como Conficker o Duqu señalan la tendencia actual de las amenazas en internet y más allá.

El Ciberespacio, por lo tanto, resulta ser un nuevo universo creado por el hombre pero que está muy lejos de estar hecho a su medida. La Humanidad necesita, curiosamente, adaptarse a su propia creación. Se trata de algo que trasciende un mero escenario de conflicto para convertirse también en uno en el que desarrollamos una parte cada vez más significativa de nuestras vidas, al que confiamos nuestros datos y nuestros ahorros y que nos ayuda a realizar nuestros sueños.

Por otro lado, el entorno cibernético es, a la vez, uno en el que nos movemos a diario y un gran desconocido. Hay muchas reticencias a abordar su tratamiento desde un punto de vista político o estratégico y existe la tendencia a confiar su gestión a soluciones técnicas que acometen sólo parcialmente los problemas que plantea. Es necesario dar un paso adelante y desarrollar una Estrategia Nacional del Ciberespacio al estilo de otros países de nuestro entorno. Una que vaya más allá del mero entorno de la Defensa y que agrupe a actores públicos y privados de aquellos sectores trascendentales para nuestra seguridad y prosperidad.

[i]

*Ángel Gómez de Ágreda**
*Teniente Coronel E.A. - D.E.M. -*

**NOTA:** Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.