LA DIMENSIÓN DESCONOCIDA

El ciberespacio es un nuevo escenario con características propias y distintivas, desafiantes y dinámicas, que obligan a una adecuación de los protocolos existentes para operar con éxito. El novel Comando Conjunto Cibernético se constituirá en el referente para llevar a cabo las tareas necesarias.

PALABRAS CLAVE: CIBERSEGURIDAD / PODER EJECUTIVO NACIONAL / MINISTERIO DE DEFENSA / MEDIDAS / TECNOLOGÍA / ESTRATEGIAS

Por **Julio Gerardo Lucero**

EL CIBERESPACIO COMO NUEVO ÁMBITO OPERACIONAL

"Un Ataque Cibernético será tomado como una declaración de guerra" expresa la Organización del Tratado del Atlántico Norte (OTAN).

Israel fue amenazado por "Anonymous"[1] con un ataque cibernético a su seguridad; un virus irrumpió las redes estadunidenses y provocó pérdidas de 3.500.000.000,00 dólares; la central eléctrica de combustible nuclear iraní de Bushehr fue atacada por un virus que destruyó el sistema de control de las centrifugas del reactor, poniéndola fuera de servicio; Estados Unidos de América creó un Comando Cibernético (USCYBERCOM[2]).

Todas estas son noticias que aparecieron en los medios, creando en muchos observadores desprevenidos cierta incredulidad, sonrisas socarronas y hasta preconceptos de amarillismos periodísticos para llenar espacio en los diarios e impactar en la opinión pública.

Si se observa la actualidad del ámbito vinculado a los acontecimientos enunciados, en la República Argentina se puede destacar el uso intensivo de la tecnología digital en la cotidianeidad y al alcance de todos, por ejemplo, realizar la compra de un contenedor de productos en Shanghái por medio de una transferencia bancaria de miles de euros, desde un banco en

El "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad" en la Argentina es un proyecto que tiene como una de sus finalidades impulsar la creación y adopción de un marco regulatorio específico.

Suiza a otro en Hong Kong, utilizando un teléfono celular desde una oficina situada en el centro de esquí de Las Leñas (Mendoza- Argentina), no es algo imposible.

Asimismo, es preciso notar que las operaciones de comercio internacional, exportaciones e importaciones de nuestro país que sumaron, en el año 2013, 157.028.000,00 dólares[3], se realizaron en su mayoría utilizando la banca electrónica, internet y redes virtuales para su concreción.

Por otro lado, la seguridad de las miles de personas que se movilizan a diario en el transporte público de nuestro país (aire, mar y tierra) se controlan, en un porcentaje significativo, con tecnología digital.

Como referencia, durante el 2012, en la República Argentina se transportaron, solo por medio aéreo, 9.557.129 pasajeros. Se añade que anualmente se realizan cerca de 14.000 millones de transacciones electrónicas en el sistema bancario nacional, principalmente por redes privadas, virtuales o Internet[4].

La creación, en el 2011, del "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad" (ICIC) en la Argentina, es un proyecto que tiene como una de sus finalidades impulsar la creación y adopción de un marco regulatorio específico que propicie protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran.

En cuanto al sector de defensa nacional, se destaca la realización de la Tercera edición del Ejercicio Nacional de Respuestas a Incidentes Cibernéticos en el destructor ARA "Almirante Brown", en cuya oportunidad el vicealmirante Marcelo Eduardo Hipólito Srur, comandante de Adiestramiento y Alistamiento de la Armada, declaró que la colaboración con el ICIC es uno de los ejes estratégicos del Ministerio de Defensa[5].

Por su parte, la Argentina y la República Federativa de Brasil profundizan estrategias en ciberdefensa, representados por sus respectivos ministros de Defensa, el ingeniero Agustín Rossi y el embajador Celso Amorim. Los dos estados, ejes del Mercosur, firmaron una declaración conjunta en la materia.

Frente a esta situación pueden surgir interrogantes como: ¿cuál es la posible evolución de las grandes tendencias en este nuevo espacio geopolítico? ¿Tienen las fuerzas armadas un rol en este escenario virtual?

Encontrar las respuestas a tales dudas motivan el esfuerzo de vencer la tendencia natural de trabajar sobre lo inmediato y pensar en la áspera incomodidad del largo plazo, para ir más allá del ahora y prepararse para el mañana incierto.

EL CIBERESPACIO

Para avanzar sobre una definición de ciberespacio, es conveniente comenzar hablando sobre Internet. Sencillamente podría definirse como "red de redes" y es también conocida, por sus usuarios, como la web o "la nube". Remonta sus orígenes a 1969, como una respuesta complementaria a las comunicaciones en los planes de defensa estadounidenses ante un ataque nuclear, y consistía en una red y subredes que permitían la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP).

De su uso militar inicial, pasó, de la mano de científicos e intelectuales, a ser un espacio de intercambio de pensamientos y conocimientos entre los miles de usuarios que se incorporaban día a día.

Esta dinámica la fue transformando, llegando, a mediados de los 80', a autoproclamarse "espacio de libertad, independencia y democracia" fuera del alcance de los poderosos. Esta primaria comunidad creía ver allí un refugio del juego milenario de las fuerzas sociales, económicas y políticas hegemónicas globales.

Varias ONG[7] de distintas nacionalidades y sustratos ideológicos, propugnan y son profetas de esta libertad.

1. *Anonymous:* es una organización informal de estructura descentralizada, sin un referente o líder, que permite cualquier irrupción o ataque informático en nombre de una causa en nombre de la libertad de Internet. Sus herramientas y métodos tienen un común denominador en cada una de las acciones atribuidas al movimiento: ataques de denegación de servicio que ponen fuera de línea a los sitios webs acceso y, en algunos casos, la intromisión y puesta en línea de información personal.
2. El USCYBERCOM planea, coordina, integra, sincroniza y conduce actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento de de Defensa y prepararse para cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los Estados Unidos y sus aliados en el ciberespacio e impedir lo mismo sus nuestros adversarios.
3. INDEC, Intercambio Comercial Argentino, Datos provisorios del año 2012 y cifras estimadas del año 2013, Buenos Aires, 2013.
4. De Nigris, A., *La bancarización en la Argentina,* Unidad de Estudios del Desarrollo - División de Desarrollo Económico, Santiago de Chile, 2008.
5. Ministerio de Defensa, MD 343, 14 de mayo de 2014. Buenos Aires, Argentina.
6. La Declaración de independencia del Ciberespacio es un texto presentado en Davos, Suiza, el 8 de febrero de 1996, por John Perry Barlow, fundador de la *Electronic Frontier Foundation* (EFF). Fue escrita como respuesta a la aprobación en 1996 de la Telecommunications Act en los Estados Unidos. El texto es una reivindicación que critica las interferencias de los poderes políticos que afectan al mundo de Internet y defiende la idea de un ciberespacio soberano.
7. ONG es la sigla de Organización No Gubernamental. Se trata de entidades de iniciativa social y fines humanitarios, que son independientes de la administración pública y que no tienen afán lucrativo.

¿Cuál es la posible evolución de las grandes tendencias en este nuevo espacio geopolítico? ¿Tienen las fuerzas armadas un rol en este escenario virtual?

Sin embargo, tal situación idealista nunca fue tan pura si se recuerda la génesis de la web y menos en estos momentos en que distintos gobiernos y organizaciones internacionales, al ver la magnitud y prospectiva de hechos irregulares como los descriptos anteriormente, consideran la necesidad de construir un orden para las actividades virtuales.

Su infraestructura tuvo una evolución vertiginosa, la incorporación de redes y computadores a la nube fue exponencial. Las estadísticas resultantes impresionan: 2.900 millones de personas (40 % de la población mundial) y 6.800 millones de dispositivos (entre algunos, PC, Smartphone, servidores) están unidos a la web[8], se envían 204 millones de mails por minuto, en la Argentina son 22 millones los usuarios que dedican un promedio de 5 horas diarias a estar conectados[9].

Todos los elementos implicados en los guarismos descriptos se encuentran inmersos en un ámbito mayor que los contiene, el Ciberespacio.

El doctor Roberto Uzal, de manera muy simple, lo define como "Internet más todas las redes, que de una forma u otra, están asociadas a ella" [10].

La existencia de este entorno creado por el hombre, ejerce influencia, cambios y nuevas ópticas en distintas áreas de pensamiento.

En una orientación más específica hacia el área de defensa, se transcribe la noción expresada por el coronel Flores:

> [El espacio cibernético es un] *Dominio operacional cuyo carácter distintivo y único está enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar, y explotar la información a través de los sistemas basados en Tecnologías de la Información y Comunicación (TIC´s) y sus infraestructuras asociadas*[11].

En lo que respecta a su morfología, los distintos modos de intercomunicación entre dispositivos, los protocolos, siguen el estándar marcado por el Modelo OSI-ISO. Esto facilita la concreción de la Web al permitir la intercomunicación entre redes y dispositivos. El modelo patrón describe 7 capas en la comunicación: Aplicación, Presentación, Sesión, Transporte, Red, Datos y Física.

Correlativamente, al reconocerse la existencia del ciberespacio se plantea la cuestión de un orden, tutela o administración del mundo virtual. De hecho el gobierno de los Estados Unidos posee cierta preeminencia en la gobernanza de la ci-

8. Unión Internacional de Telecomunicaciones (ITU) *ITU International Telecommunication Union.* Rescatado de *http://www.itu.int/net/pressoffice/press_releases/2013/41-es.aspx#.U7WkCIcU8cA*
9. Diario *Clarín.* Rescatado de *http://www.ieco.clarin.com/tecnologia/estadisticas-Internet-millones-enviados-minuto_0_1167483520.html., 25 de julio de 2014.*
10. Uzal, Roberto, 21 de mayo de 2014. Buenos Aires, Argentina.
11. Flores, H., *Los ámbitos no terrestres en la guerra futura: Ciberespacio,* Gabinete de Estrategia Militar, Madrid, 2011.

bercomunidad, al tener en su Administración Nacional de Telecomunicaciones e Información la asignación/coordinación a nivel global de las "direcciones IP"[12] para desarrollarse en la virtualidad, función que efectúa a través de la organización *Internet Assigned Numbers Authorit*y (IANA).

Llamativamente, los Estados Unidos declararon, recientemente, su intensión de resignar, unilateralmente, este privilegio, sin decir a quién tiene previsto dejárselo[13]. Esa posible modificación fue el origen de distintas reuniones, la más reciente de ellas, organizada por el gobierno de la República Federativa del Brasil, Net-mundial[14], a la que asistieron representantes de la Cancillería Argentina y donde quedaron definidas dos tendencias para la futura gobernanza de internet: la de cooperación y la del consenso[15].

Asimismo, se discutió sobre los conflictos y su posible solución. En lo referente al encuadre legal para responder las acciones contra los estados, en este nuevo escenario, la postura de amplia anuencia es el artículo 51 de la carta de la ONU, "Legítima Defensa".

En lo concerniente a resolución de conflictos, contó con amplio asentimiento al esquema participativo que se utilizó ante el ataque a las plataformas petroleras iraníes, con el virus Flame (mayo 2012): La *Nación Agredida* denunció el hecho ante la *ONU/"Unión Internacional de Telecomunicaciones,* y esta última envió inspectores para analizarlo y que se emitiera a una declaración.

Ya a esta altura se puede considerar seriamente un nuevo ámbito de posibles fricciones, fuertemente "asimétrico" y antropotécnico, al alcance de las acciones de actores estatales y no estatales[16].

Desde la óptica de la Geopolítica Crítica[17] y, en forma genérica, se puede tomar la libertad de catalogar al Ciberespacio como un espacio geopolítico sujeto al juego de poderes, intereses e influencias de particulares, organizaciones y estados[18].

LA ESTRATEGIA

La nueva esfera bajo análisis esconde una íntima trama de gran complejidad donde, de acuerdo con la faceta desde la cual se la observe, se entrelazan intereses nacionales que pueden potenciarse o verse limitados por las posturas que se adopten.

Desde la óptica de la Geopolítica Crítica y, en forma genérica, se puede tomar la libertad de catalogar al Ciberespacio como un espacio geopolítico sujeto al juego de poderes, intereses e influencias de particulares, organizaciones y estados.

Hoy en el área virtual de la República Argentina se podría decir que existe un *status quo* en lo que atañe a las acciones irregulares de magnitud.

Esta situación, no obstante, no debe llamar a la inacción, pues la prospectiva de los hechos e incidentes internacionales llevan a suponer que el equilibrio se verá alterado en el mediano y largo plazo. La evolución proyectada por los grandes actores internacionales avizoran un evento catastrófico que denominan "Gran Meteorito" (un 11 de septiembre cibernético). Este "ataque" definirá un antes y un después en las relaciones de poder en el Ciberespacio.

Tales augurios y su posible evolución motivan la elaboración y puesta en práctica de una estrategia defensiva del patrimonio nacional en el nuevo ámbito que permita la alineación de recursos hacia los fines que se determinen en el área, sustentado, con un modo de razonamiento estratégico descendente, la protección de los intereses nacionales.

El Poder Ejecutivo Nacional está tomando medidas de defensa en la virtualidad. El germen se localiza en la Oficina Nacional de Tecnología de la Información (ONTI) a través del ya mencionado ICIC.

La situación actual convierte a los factores económicos en limitantes de los procesos de modificación/adecuación de infraestructuras y, si sumamos el carácter voluntario de las recomendaciones del Programa para la Circunscripción Privada, originan una multiplicidad de situaciones que carcomen la integridad de una estrategia general protectora ante posibles amenazas.

El Ministerio de Defensa tiene como uno de sus lineamientos el desarrollo de la seguridad de los sistemas de información

12. Este número es la puerta de entrada al Ciberespacio, le da una identidad al dispositivo que opera en él, sin este su ingreso y tarea en el mismo es imposible.
13. Avni, B., *Newsweek*. Rescatado de *http://www.newsweek.com/2014/04/04/obama-wants-global-community-run-internet-it-could-end-hands-china-or-putin-248037.html*
14. Llevada a cabo en San Pablo Brasil, entre el 23 y 24 de abril de 2014. Contó con la asistencia de representantes ministeriales de 12 países (Argentina, Brasil, Francia, Ghana, Alemania, India, Indonesia, Sudáfrica, Corea del Sur, Túnez, Turquía y los Estados Unidos de América) y 12 miembros de la comunidad internacional de múltiples partes interesadas. Este comité cuenta con representantes de la Unión Internacional de Telecomunicaciones (UIT), del Departamento de Asuntos Económicos y Sociales (DESA) de las Naciones Unidas y de la Comisión Europea.
15. *Net Mundial References.* Rescatado de *http://netmundial.br/wp-content/uploads/2014/04/NETmundial PublicConsultation-FinalReport20140421.pdf*
16. Ballesteros Martín, M. A., "La evolución de los conflictos", *Panorama geopolítico de los conflictos 2013- Instituto Español de Estudios Estratégicos*, 12, Madrid, enero de 2014.
17. Rodríguez Garoz, R., "Scripta Nova", *Revista Electrónica de Geografía y Ciencias Sociales.* Rescatado de *http://www.ub.edu/geocrit/sn/sn-198.htm.* Una adaptación de la idea de espacio desde una perspectiva de la Geopolítica Crítica. La Geopolítica Crítica se ocupa de estudiar el espacio planetario y sus modos de producción y reproducción, para lo cual sería necesario ver la interconexión de elementos económicos, políticos, simbólicos e institucionales o legales en la práctica humana histórica concreta, aceptando la espacialidad de los hechos sociales. Afronta un análisis histórico de los discursos y prácticas de los Estados.
18. Koutuodjian, A. entrevista de J. Lucero, 14 de mayo de 2014.

específicos de las fuerzas armadas y, por tal razón, se creó, el 14 de julio de 2014, el Comando Conjunto de Ciberdefensa.

A manera de síntesis se puede describir la evolución de un acontecimiento hipotético en el marco actual: ante una acción cibernética irregular que busque la interrupción o destrucción de elementos de un sistema vital (plantas generadoras de energía eléctrica, petroquímicas, centrales nucleares, control de tránsito aéreo), estos organismos tendrán, en forma individual, el mayor peso de la detección, identificación y neutralización primarias de las amenazas a sus redes y sistemas.

REPENSAR LA ESTRATEGIA: ROL Y CAPACIDADES DE LAS FUERZAS ARMADAS

Como espacio geopolítico, el ciberespacio puede dar lugar a teorías y conceptos de la ciencia geopolítica. Sobre esta base podemos aplicar, por analogía, los argumentos de Juan Recce sobre "Ocupación Científica del Espacio"[19] y asociar la proyección estratégico-espacial argentina en la virtualidad de interés nacional, al desarrollo tecnológico.

Para ello, la avanzada sobre este nuevo ámbito podría ser un organismo dual (por ejemplo: combinado entre CONICET[20] y Ministerio de Defensa) que encarne un proceso de innovación tecnológica articulador de las capacidades del Complejo de Ciencia y Tecnología del país con la estructura logística propia de las fuerzas armadas.

Si se opta por ese replanteo, es conveniente que el ente ejecutor esté en condiciones de sostener y mantener una condición de alerta estratégica ante la evolución de amenazas que requieran un mayor control, siempre con un modelo de defensa y con un claro rechazo y oposición a políticas, actitudes y capacidades ofensivas de proyección de poder a terceros estados.

Hoy, en caso de una escalada potencial de un conflicto, las diversas "capas" de la protección estatal responderían de acuerdo con el origen de la misma, evaluando si entra en la jurisdicción de defensa o de seguridad, en el marco naturalmente complejo del asunto, con un vital tiempo de reacción que aún no está totalmente definido debido a las novedosas características que presenta el espacio cibernético.

El Libro Blanco de la Defensa define como un interés estratégico el dominio del ciberespacio, no sólo para el ejercicio del comando y control y para el funcionamiento en las redes de los sistemas de defensa, sino también para repeler y conjurar amenazas militares estatales externas que puedan producirse utilizándolo como vía de ejecución o teniéndolo como objetivo[21]. Indudablemente esto habilitaría a la Defensa a estar en capacidad de contribuir a su mejor logro.

Necesariamente, la evolución probable hacia una participación de las fuerzas armadas en un servicio nacional de alerta estratégico de amenazas cibernéticas, enlazaría la necesidad de la consideración particular de la posible tarea con el Ciclo

19. Recce, Juan, *Fundación Argentina Ase.* Rescatado de Atlantium: *http://argentinaase.org/atlantium/*
20. Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) es el principal organismo dedicado a la promoción de la ciencia y la tecnología en la Argentina. Su actividad se desarrolla en cuatro grandes áreas:
    - Ciencias agrarias, ingeniería y de materiales
    - Ciencias biológicas y de la salud
    - Ciencias exactas y naturales
    - Ciencias sociales y humanidades
21. Ministerio de Defensa, Argentina, *Libro Blanco de la Defensa,* 2010, p. 48.

En caso de una escalada potencial de un conflicto, las diversas "capas" de la protección estatal responderían de acuerdo con el origen de la misma, evaluando si entra en la jurisdicción de defensa o de seguridad.

de Planeamiento de la Defensa Nacional a través de la Directiva Política para la Defensa Nacional (DPDN). Este documento prevé una apreciación del escenario de defensa y seguridad que identifique tendencias, riesgos y amenazas a los intereses nacionales para el mediano y largo plazo[22].

El diagnóstico actual de la DPDN disponible al público e investigadores no incluye expresamente el escenario bajo análisis, situación que se estima que sufrió una modificación ante la creación del Comando Conjunto de Ciberdefensa.

Más allá de las consideraciones formales, la complejidad del escenario planteado exige una atención especial en la construcción de un conocimiento epistemológicamente seguro acerca del ciberespacio, lo cual requiere recursos humanos específicamente formados, información y tiempo.

El potencial rol de las fuerzas armadas puede analizarse en tres niveles, asociables al corto, mediano y largo plazo.

En el corto plazo, las fuerzas armadas podrían ejecutar una tarea de presencia en el ciberespacio de acuerdo con el alcance que defina el Ministerio de Defensa.

Es decir, colaborando o participando en un Servicio de Alerta Estratégica, focalizado en la identificación de posibles ataques y su origen (problema de atribución[23]), con la tecnología de "Análisis de Flujos de Redes"; proceder que respeta el mandato legal de resguardar la privacidad de los usuarios de la web[24].

Asimismo, efectivizar una presencia implicaría emitir a la cibercomunidad un mensaje estratégico de compromiso con la protección de los intereses argentinos en este ámbito.

En el mediano plazo, el objetivo sería tender a la concreción formal de un acuerdo de cooperación en el ámbito regional para formalizar las actividades conjuntas de respuestas a incidentes cibernéticos que ya se realizan con naciones amigas, como la brasileña. La creación de un frente regional común aumenta la disuasión de cada uno de sus integrantes a las acciones irregulares[25].

Ya en el largo plazo, considerando el crecimiento en cantidad e importancia de los sistemas críticos, es recomendable detallar un protocolo para las fuerzas armadas frente a las potenciales amenazas de otros estados que pretendan alterar el normal desarrollo de la actividad virtual de incumbencia nacional y regional, equiparándolo con la respuesta esperada en las dimensiones operacionales clásicas.

Incorporar una nueva capacidad implica la obtención de medios, el desarrollo de una doctrina y procedimientos de empleo, además del fundamental adiestramiento.

CONCLUSIONES

Al analizar la virtualidad no debemos caer en la trampa de la seducción de lo simbólico y olvidar que mucho es apariencia[26]. El ciberespacio es un nuevo escenario que tiene características propias y distintivas que obligan a una adecuación de los protocolos existentes para operar con éxito en él.

La seguridad en esta dimensión depende no solo de la existencia de medios defensivos, sino también de la capacidad de saber que sucede en él, de modo tal de no ser sorprendido por incidentes irregulares. El escenario de un ciberconflicto está caracterizado por su originalidad desafiante y dinámica, lo que lleva a un proceso continuo y perseverante de aprendizaje para lograr y mantener efectividad. El novel Comando Conjunto Cibernético será el referente en estas tareas.

Es posible transitar el camino de la Apropiación Científica del Ciberespacio en un trabajo dual bajo el control del Estado Argentino, sustentado en un cambio de paradigma que, por medio de la Ocupación Científica del Espacio, logre una posición relativa favorable de la región, tanto para la discusión de la gobernanza del ciberespacio, como también para el ingreso a un universo de oportunidades posibles para las futuras generaciones que tiene como límite solo la imaginación.

El impulso a la Ciencia y la Tecnología iniciado por el Plan Nacional de Ciencia, Argentina Innovadora 2020, genera un marco estratégico, político y social propicio para avanzar en la vinculación de Ciencia, Tecnología, Defensa y Desarrollo Económico[27].

Existen opiniones que están en contra de cualquier participación del estado como ente de control en el mundo virtual, asignando la responsabilidad de su seguridad/defensa individual a la persona física o jurídica que operan en ese ambiente.

Tal postura, en la práctica, lleva a delegar la defensa de un

22. Poder Ejecutivo Nacional, Argentina, Decreto 1729/07. *Directiva de Política de Defensa Nacional,* Ciudad Autónoma de Buenos Aires, 11 de noviembre de 2007.
23. Garau Pérez-Crespo, C., "El twiter de Sun Tzu", *Revista General de Marina,* 631, 2014. El Problema de la Atribución: es la dificultad de identificar de forma positiva al autor de los ataques, representa el 85 % de las posibles amenazas y su aspecto más destacado es el trastorno que representa para el tratamiento legal y jurisdiccional de los ciberataques, así como la posible consideración de la acción ofensiva bajo el prisma del derecho de la guerra.
24. Uzal, Roberto, 21 de mayo de 2014. Buenos Aires, Argentina.
25. Uzal, Roberto, 21 de mayo de 2014. Buenos Aires, Argentina.
26. Anta, J. L., y Palacios, J., *Revista Investigaciones Sociales,* año IX, N° 15. L. 2. UNMSM / IIHS, Ed., Jul-Dic 2005. Rescatado de *http://scholar.google.com/scholar_url?hl=es&q=http://revistasinvestigacion.unmsm.edu.pe/index.php/sociales/article/download/7007/6201&sa=X&scisig=AAGBfm1wg0ICZL50slJcyyt4noTl0u6bdFw&oi=scholaralrt*
27. Ministerio de Ciencia, Tecnología e Innovación Productiva, *Plan Nacional de Ciencia, Tecnología e Innovación:* Argentina Innovadora 2020. Rescatado de *http://www.argentinainnovadora2020.mincyt.gob.ar/?page_id=312*

Julio Gerardo Lucero
Comodoro de la Fuerza Aérea Argentina. Oficial de Estado Mayor. Ingeniero de Sistemas. Licenciado en Sistemas Aeroespaciales y Magíster en Administración de Sistemas de Información. Egresó de la Escuela Superiorde Guerra Conjunta en el 2014 del Curso Conjunto de Estrategia y Conducción Superior. Actualmente se desempeña como Jefe del Grupo Capacitación Técnico Profesional de la Escuela de Suboficiales de la Fuerza Aérea.

ataque cibernético que puede inutilizar una destilería petrolera (sistema crítico), tal como ocurrió en el caso Bushehr-Irán, a la empresa misma. Por el absurdo, entonces, podemos suponer que la defensa de un ataque aéreo contra la misma destilería y con el mismo objetivo, su inutilización, también sería responsabilidad de la empresa.

Una estructura de defensa en el Ciberespacio no implica un obligado atentado a las libertades individuales, ya que tecnológicamente es posible ejercer una protección efectiva y de acuerdo a normas legales si se limitan los trabajos a los estratos de la "Nube" que no involucran la información privada, es decir, si se trabaja sobre las capas: Física, Datos y Red del modelo OSI-ISO[28].

Conceptual y operativamente se podría considerar al ciberespacio como un macro sistema en el cual, a través de diferentes tecnologías, los estados deberían controlar y supervisar las acciones que se efectúan de forma tal de saber si se ajustan a derecho, acuerdos sociales y/o comerciales y, a su vez, para corroborar que no amenazan los intereses nacionales.

Si se parte de la premisa que el ambiente ciberespacial de interés nacional es uno, este debe ser abordado como una unidad integral. Por lo tanto, es recomendable propiciar la constitución de una autoridad ciberespacial ejecutiva, a nivel nacional, que vele por los intereses argentinos y aúne los esfuerzos estatales y privados contra el accionar de actores indeseados.

En este sentido, los organismos de coordinación creados y en funcionamiento, como así también las acciones llevadas a cabo por los ministerios y secretarías, son contribuyentes al logro de ese fin.

Las fuerzas armadas, por el poder que administran, son comandadas por el Jefe de Estado. Representan la última herramienta para asumir la defensa de la nación contra un enemigo militar externo. Son instrumentos que el estado tiene a su disposición para ejercer la plena defensa de sus intereses vitales. Como parte del Estado Argentino y subordinado a sus autoridades legítimas, ocupan el rol definido por éstas en la temática tratada.

No obstante, la tarea ya asignada de brindar seguridad a sus sistemas de información propios puede ser complementada con un estado de Alerta Estratégico, en el marco de una Actitud Estratégica netamente defensiva, a los efectos de colaborar en lograr un oportuno tiempo mínimo de reacción ante los ataques a los sistemas críticos.

Sólo una estrategia creativa e integral permitirá neutralizar los efectos perjudiciales de las acciones irregulares en el Ciberespacio. La inacción o la mera reacción a los estímulos estratégicos generados por otros actores no son suficientes, hipotecan nuestra iniciativa y comprometen la posibilidad de que las generaciones futuras dispongan de la libertad de acción necesaria para su desarrollo y felicidad.

Uzal, Roberto, 21 de mayo de 2014. Buenos Aires, Argentina.