Escuela Superior de Guerra Conjunta de las Fuerzas Armadas

Tema.

OPERACIONES CIBERESPACIALES

Título.

DESAFÍOS OPERACIONALES EN EL CIBERESPACIO COMO NUEVO CAMPO DE LUCHA

Trabajo Final Integrador

Mayor EZEQUIEL H. RODRÍGUEZ CISNEROS

2012

Aclaración

Las opiniones, análisis e interpretaciones expresadas en el presente trabajo académico son exclusivos del autor, y no reflejan necesariamente políticas oficiales ni posición, tanto de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas como de la Fuerza Aérea Argentina.

TRABAJO FINAL INTEGRADOR

RESUMEN

Entre las transformaciones del mundo actual, la universalización del discurso informático y la interdependencia global a través de redes digitales, ha dado lugar a un nuevo ámbito de realidad, el Ciberespacio.

La doble condición de éste ámbito, ser al mismo tiempo motor de desarrollo socioeconómico, y factor de vulnerabilidad en las áreas de seguridad y defensa, plantea desafíos que ameritan ser investigados.

Por otra parte, esto demanda de cada país, el diseño de nuevos instrumentos militares y fuerzas especialmente adiestradas para realizar operaciones militares ciberespaciales, que atiendan a las características específicas y disímiles de este nuevo ámbito.

Se han explorado diversas concepciones generales acerca del Ciberespacio; identificado actores relevantes, determinado las condiciones de producción de las nuevas operaciones ciberespaciales, y formulado algunos desafíos operacionales en este nuevo ámbito para el caso particular de la Republica Argentina.

Asimismo, pudo reconocerse que la hipótesis que nos planteamos, ha sido refutada; y de tal manera, encontramos que los desafíos operacionales en el Ciberespacio dentro del ámbito de la República Argentina, ya han comenzado a establecerse, y al mismo tiempo, los actores involucrados perciben como un beneficio la realización de operaciones ciberespaciales.

PALABRAS CLAVE

Ciberespacio, redes, operaciones militares, información y comunicación.

Tabla de Contenidos

INTRODUCCIÓN

Entre los cambios más espectaculares y permanentes que ha experimentado la humanidad en su historia, podemos mencionar el del área de las comunicaciones, que ha sido producto del desarrollo de la tecnociencia contemporánea y ha revolucionado la velocidad del intercambio de información.

El constante y exponencial cambio de las nuevas tecnologías, atraviesa transversalmente a la sociedad, y produce efectos significativos en la forma de vida, el trabajo y el modo de entender el mundo por parte de los sujetos.

Sin lugar a dudas, el proceso de adaptación a dichos cambios no ocurre sin dificultades, y las instituciones militares no están ajenas a ello.

Deteniéndonos en estas últimas y en sus características propias, encontramos que las mismas, han poseído una gran dificultad para procesar los cambios de paradigmas en general, y particularmente, el cambio que hubo en el paradigma de los objetos desde la era industrial a la era de la información.

En esta última, y gracias a las Tecnologías de la Información y la Comunicación, el movimiento de la información se volvió más rápido que el movimiento físico.

Reflexionar respecto de esta realidad, nos permitió valorar la necesidad de aproximarnos al tema del Ciberespacio, ya que éste, es el ámbito en donde la información, en muchos casos se genera y, en todos, se moviliza, excediendo ampliamente a la dinámica propia de los objetos físicos.

Esta revolución tecnológica se ha caracterizado por la emergencia de una estructura social en red, en todos los ámbitos de la actividad humana, y con la interdependencia global de dicha actividad, conllevando un proceso de transformación multidimensional.

Cómo entonces, habríamos de mantenernos al margen de semejante transformación de nuestro entorno sin abocarnos siquiera, a investigar las implicancias en los asuntos militares, y más precisamente, en las posibilidades de definir y efectuar operaciones militares en y a través del Ciberespacio.

El Ciberespacio entonces, definido como un nuevo ámbito para efectuar operaciones militares, plantea un sin número de interrogantes. Por ello en esta primera aproximación, nos preguntamos: ¿cuáles son los desafíos operacionales que presenta el

Ciberespacio como nuevo campo de lucha?

Entendemos que la composición heterogénea del Ciberespacio, que requiere la emergencia de un nuevo ámbito operacional y la elevada complejidad que supone el análisis de los casos de intervención, implican la posibilidad de una participación directa de muchas más disciplinas de las que podría abarcar cualquier investigador.

Por lo tanto, cabe aclarar que, el recorte necesario que limita al presente estudio, no es a los fines de simplificar la mirada sobre el objeto, sino condición de posibilidad para volverlo asible.

El estudio estará limitado al campo disciplinar militar, y específicamente al nivel operacional.

A su vez, y aunque el Ciberespacio no posea fronteras estatales o físicas, constreñiremos el alcance del objeto de investigación al análisis del Ciberespacio en la República Argentina.

Dada la característica del objeto de estudio, las experiencias que se recogen han sido prácticamente todas analizadas desde la perspectiva del nivel estratégico, realizadas por actores estatales, generalmente grandes potencias, y en idioma inglés.

Por el contrario, el análisis del objeto de estudio desde la perspectiva del nivel operacional, y realizado por Estados emergentes, aún no ha sido extensamente efectuado. Al mismo tiempo, encontramos que la producción en idioma español sobre esta temática es escasa. Pensamos entonces, que el presente estudio podrá contribuir a la comprensión del complejo ámbito de lucha que constituye el Ciberespacio, desde la perspectiva del nivel operacional de la guerra, y desde la particular mirada de sujetos de cultura hispanohablantes.

Al mismo tiempo esperamos colaborar para abrir nuevas líneas de investigación en torno a la ciberguerra en la República Argentina.

En el presente trabajo hemos planteado como objetivos particulares explorar los actores -o redes de actores- que estén involucrados en el Ciberespacio en el caso particular de Argentina; y determinar las condiciones de producción de las nuevas operaciones militares en el Ciberespacio.

La hipótesis es que los desafíos operacionales en el Ciberespacio, dentro del ámbito de la República Argentina no han sido establecidos, y al mismo tiempo, los actores involucrados no perciben como un beneficio la realización de operaciones ciberespaciales.

El diseño metodológico hace del presente trabajo una investigación cualitativa de carácter descriptivo, con análisis documental de fuentes primarias y secundarias, como documentos disponibles en línea, páginas web, periódicos, y manuales vigentes.

En el presente trabajo recorreremos, en el primer capítulo, algunas consideraciones sobre la naturaleza del Ciberespacio; los tipos y niveles de comunicación que se desarrollan en el; la definición del término; los dilemas del Ciberespacio; los límites del ambiente ciberespacial; y la estructura física del sistema.

En el segundo capítulo, centraremos nuestra atención en la estructura física del sistema en Argentina; los actores involucrados; algunas consideraciones sobre el Ciberespacio como nuevo ámbito de lucha; el marco legal; y las operaciones militares en el Ciberespacio.

CAPITULO I. ¿QUÉ ES EL CIBERESPACIO?

I.1 Algunas consideraciones sobre su naturaleza

En 1984 William Gibson, autor estadounidense nacido en 1948, publica la novela Neuromante (Neuromancer, en su título original inglés).

Hoy, luego de casi cuarenta años de la aparición de la novela de Gibson, y tras enormes cambios culturales y avances tecnológicos, una de las primeras dificultades que hemos encontrado para la consecución del presente trabajo, gira entorno a la mismísima palabra *Ciberespacio*, ya que ésta no remite a un significado unívoco, y su definición depende, entre otras variables, de la perspectiva, cultura, idioma y conocimiento de quien intenta abordar su definición.

Indudablemente, el mayor aporte, no siempre acreditado, de Neuromante es el término *Ciberespacio*, acuñado por Gibson (2001) y utilizado por vez primera en dicha obra. La definición que allí se lee del mismo es la siguiente:

"Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información. Como las luces de una ciudad que se aleja..."[1]

Paralelamente a sus atributos literarios, lo que Gibson despliega es una asombrosa intuición anticipatoria respecto de algunos de los más impactantes e inesperados cambios que, en materia cultural y tecnológica, ocurrieron a nivel global desde mediados de la década de los ochenta.[2]

Pero la introducción indirecta de un término recogido de un ámbito literario, ha hecho que su aplicación no sea, muchas veces, lo suficiente precisa a la hora de manejarlo.

Es así que, por ejemplo, para el Departamento de Defensa de los Estados Unidos de Norteamérica, el Ciberespacio es *"un dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos,*

[1] Gibson, William. 2001. Neuromante. Barcelona. Ediciones Minotauro. Octava reimpresión. 69-70.
[2] Alatorre Cuevas, Israel. Neuromante: el futuro que llegó. número 25 de la revista: "Tramas, Subjetividad y Procesos Sociales", publicación de la Universidad Autónoma Metropolitana plantel Xochimilco.

procesadores y controladores integrados."[3]

Dentro de la comunidad de Tecnologías de la Información y Comunicaciones (TIC) el Ciberespacio se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos.[4]

El Ciberespacio, puede también definirse como un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas.[5]

Según Rain y Lorents (2010) el Ciberespacio es un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El Ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física.[6]

La Comisión Europea define vagamente al Ciberespacio como el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo.[7]

Para la Unión Internacional de Telecomunicaciones (UIT), el *"…Ciberespacio está integrado por cientos de miles de servidores, ordenadores, encaminadores, conmutadores interconectados y sistemas de transporte de la información (cables, satélites, medios radioeléctricos) que permiten un funcionamiento armonioso de las infraestructuras básicas."*[8]

Dan Kuehl (2009) respecto de la definición del término afirma: *"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 las Tecnologías de Información y Comunicaciones (TIC) y también sus infraestructuras asociadas."*[9]

Para Aguirre Romero (2004) *"el Ciberespacio existe solamente como espacio*

---

[3] Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms.
[4] Fojón, Enrique y Sanz, Ángel. "Ciberseguridad en España: una propuesta para su gestión", Análisis del Real Instituto Elcano, ARI Nº 101/2010
[5] Rain, Ottis y Lorents, Peeter. "Cyberspace: Definitions and Implications", Cooperativa Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.
[6] Definición extraída del glosario de términos informáticos, Whatis. Enlace: http://searchsoa.techtarget.com/definition/cyberspace. Fecha de consulta 15-9-2012.
[7] European Commission. Glossary and Acronyms (Archived). In Information Society Thematic Portal, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. Fecha consulta 15-9-2012.
[8] Unión Internacional de Telecomunicaciones (UIT). Comisión de Estudio 2-3er Periodo de Estudios (2002-2006) "Informe sobre las infraestructuras nacionales de seguridad del ciberespacio" Ginebra 2006.
[9] Kuehl, Dan. From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management College-National Defense University, Estados Unidos, 2009.

relacional; su realidad se construye a través del intercambio de información; es decir, es espacio y es medio. Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes…""…el Ciberespacio surge en y por la comunicación, de ahí su doble naturaleza de espacio y medio. Es, por tanto, un espacio que se genera cuando se producen ciertos tipos de comunicación."[10]

I.2 Realidad, Virtualidad, Ficción[11]

Para comprender la naturaleza del Ciberespacio es esencial identificar la diferencia entre espacio físico y espacio virtual.

Si entendemos como real un mundo en el que es posible realizar acciones y tomar decisiones, lo virtual no es lo imaginado/imaginario, como sucede con lo ficticio, sino que es un espacio generado en el acto de comunicación.

La aparición de lo virtual no es fruto de un desajuste interno de la percepción, sino de la construcción, deliberada y consciente, de un nuevo espacio en el que nos desarrollamos como humanos.

Este espacio virtual está constituido, básicamente, por la ampliación de nuestra capacidad de comunicación, es decir, de interacción.

La base de este espacio virtual y relacional, punto de encuentro, lugar de convivencia, es la comunicación, el intercambio de información.

Esta capacidad de interactuar se ve también ampliada respecto a otras formas anteriores más limitadas, y por ello, para comprender su especificidad, es necesario analizar las formas de comunicación que permite.

I.3 Tipos y niveles de comunicación en el Ciberespacio[12]

En el Ciberespacio, las comunicaciones que se establecen son básicamente de tres tipos: a) las relaciones de intercambio de información entre máquinas; b) las relaciones de intercambio de información entre hombres y máquinas; y) las relaciones de intercambio de información entre seres humanos a través de las máquinas.

Estos tres tipos de intercambios de información no deben pensarse como elementos separados. La realidad es que en el Ciberespacio quienes se comunican

[10] Joaquín Mª Aguirre Romero 2004. Espéculo. Revista de estudios literarios. Universidad Complutense de Madrid. http://www.ucm.es/info/especulo/numero27/cibercom.html
[11] Ídem.
[12] Ídem.

directamente son las máquinas. Son ellas las que actúan como mediadoras para posibilitar nuestras comunicaciones interpersonales.

El Ciberespacio es un espacio relacional cibernético, en el que máquinas, que constituyen redes, sirven de medio para que se establezcan comunicaciones entre humanos.

El hecho es que estos tres tipos de comunicaciones se dan simultáneamente, formando parte de un proceso: para establecer contacto con otros seres humanos que están en otros puntos de la red, nosotros nos comunicamos con las máquinas, que se comunican entre sí.

Sin embargo, el utilizar el término "comunicación" tanto para máquinas como para hombres, o entre hombres y máquinas, puede inducirnos a error si pensamos que estos procesos de intercambio de información son de la misma naturaleza.

Efectivamente, en los tres casos se produce un intercambio de información, pero estos tienen fines y condicionantes distintos. Los fenómenos de intercambio de información se dan prácticamente en todos los niveles de la escala biológica y es la forma de regulación o de autorregulación de los sistemas complejos. Pero lo que nos interesa en este momento son dos tipos de fenómenos de intercambio y su naturaleza: los que se producen entre seres humanos y máquinas, y la interrelación entre humanos.

Son cada vez más las zonas de equivalencia o las sustituciones de actividades entre ambos mundos. Ciertas tareas que antes era necesario realizar físicamente, ahora se pueden realizar a través de escenarios virtuales alojados en el Ciberespacio. En muchos casos, la eficacia del mundo virtual ha hecho desaparecer del mundo real elementos que no hace mucho parecían firmemente anclados en nuestro entorno material.

I.4 Definición del término

Como habrá percibido el lector hasta aquí, no hay acuerdo respecto a la definición del término *Ciberespacio*, por ello, y a los fines de orientar el presente trabajo, hemos construido un concepto a partir de la combinación de ideas de diversos autores citados precedentemente. Fijaremos entonces, como definición de Ciberespacio a la siguiente:

> *Espacio relacional que se construye a través del intercambio de información constituido sobre los sistemas de Tecnologías de Información y Comunicaciones (TIC).*

Una característica fundamental del Ciberespacio es que la actividad que se realiza en el se operacionaliza a través de una realidad virtual, no asible materialmente, aunque, al menos hasta ahora, las acciones se originen y/o recepcionen desde componentes

físicos.

Lo sorprendente, es que las acciones que se realizan en esa realidad digital y virtual, pueden producir cambios en el mundo real y material, y en muchos casos inclusive, ocasionar daños considerables.

Así como, el Ciberespacio se ha constituido en el sistema nervioso de los sistemas de control de las infraestructuras críticas de un Estado[13]; y brinda a la sociedad, entre otras cosas, la posibilidad de disfrutar de comunicaciones y redes sociales en cualquier momento y desde cualquier lugar, tener acceso a información prácticamente ilimitada, socializar con personas de todo el mundo, comparar y adquirir servicios y productos; por otro lado también, se ha constituido como un ámbito que otorga la posibilidad de ser utilizado para producir acciones hostiles, amenazas o agresiones.

A éstas últimas se las puede clasificar en tres tipos, en función de quien realice la acción:[14]

Cibercrimen: cuando son individuos o grupos no estatales los que utilizan el Ciberespacio para cometer actos ilícitos en beneficio propio; por ejemplo: suplantación de identidad para acceder a cuentas bancarias. En general estas acciones son reconocidas como delitos y de incumbencia policial.

Ciberterrorismo: cuando quienes lo realizan son individuos o grupos no estatales que, a través del Ciberespacio, buscan efectos de naturaleza variable sobre individuos, empresas e incluso Estados. Los medios para hacer frente a estas acciones variarán según sea el marco legal del Estado considerado.

Ciberguerra: Estado o grupos de Estados que atacan la estructura funcional y/o decisional de otro u otros Estados, empleando el Ciberespacio, y normalmente, junto al empleo de capacidades cinéticas tradicionales.

I.5 Los Dilemas del Ciberespacio

Los principales dilemas entorno al Ciberespacio son dos: seguridad versus respeto de libertades individuales; y vulnerabilidad versus desarrollo tecnológico.

Respecto al primer dilema, nos encontramos frente a la confrontación de paradigmas que abogan por lograr un mayor control del Ciberespacio que devenga en un

[13] Unión Internacional de Telecomunicaciones (UIT). Comisión de Estudio 2-3er Periodo de Estudios (2002-2006) "Informe sobre las infraestructuras nacionales de seguridad del ciberespacio" Ginebra 2006. Pág. 1.
[14] Centro Superior de Estudios de la Defensa Nacional. Ministerio de Defensa Español. "Los Ámbitos No Terrestres En La Guerra Futura: Espacio". 2012.

ámbito mas seguro, y el tendiente a mantener al Ciberespacio como un ámbito desregulado y libre del control del poder hegemónico.

En definitiva, el problema discurre entre la necesidad de proteger las redes y los servicios de información, y a su vez, proteger las libertades individuales inherentes a sociedades democráticas, en especial la libertad de expresión y la protección de la intimidad.

Respecto al segundo dilema, surge del grado de desarrollo y dependencia que tenga el Estado de sistemas tecnológicos e informatizados, ya que la gravedad de los efectos que puede provocar un ataque cibernético en un Estado con un elevado desarrollo y dependencia de este ámbito, es mucho mayor que la afectación que puede recibir un Estado cuya estructura organizacional y decisional no se sustenta en capacidades ciberespaciales que puedan ser atacadas.

I.6 Límites del ambiente ciberespacial

Desde una perspectiva sistémica, el Ciberespacio se constituye como un espacio diferenciado respecto de un entorno. Esta diferencia es la que se establece entre el mundo *real* respecto a un mundo *virtual*. Concebido el Ciberespacio como *sistema*, el mundo real se constituye como su entorno diferencial. Niklas Luhmann (1998) señala:

"El punto de partida de cualquier análisis teórico-sistémico debe consistir en la diferencia entre sistema y entorno [...] Los sistemas están estructuralmente orientados al entorno, y sin él no podrían existir: por lo tanto no se trata de un contacto ocasional ni tampoco de una mera adaptación: Los sistemas se constituyen y se mantienen mediante la creación y la conservación de la diferencia con el entorno, y utilizan sus límites para regular dicha diferencia. Sin diferencia con respecto al entorno no habría autorreferencia ya que la diferencia es la premisa para la función de todas las operaciones autorreferenciales. En este sentido, la conservación de los límites (boundary maintenance) es la conservación del sistema."[15]

Tal como indica Luhmann, el hecho diferencial es la base, el punto de partida, para la comprensión de un sistema. En los supuestos teóricos de Luhmann, identidad y diferencia son los dos principios básicos en la determinación del sistema. Ambos principios son necesarios y complementarios: es la diferencia la que permite alcanzar la identidad frente al entorno.

[15] Niklas Luhmann (1998 2ª): Sistemas sociales. Lineamientos para una teoría general. Barcelona, Anthropos, p. 40

En el Ciberespacio nos encontramos ante un sistema con una doble condición: su base material (redes, hardware, etc.) y su uso social (usuarios, relaciones y procesos).

Olvidar esta doble condición puede producir múltiples errores conceptuales y de percepción.

El Ciberespacio es, entonces, un sistema social constituido sobre un sistema tecnológico, y las posibilidades emergentes del primero están en función de los desarrollos que se dan en el segundo.

Dicho de otro modo, la tecnología, entendida como arquitectura material del sistema, es la que posibilita el establecimiento de los tipos de interacciones entre los elementos que constituyen el sistema social.

De esta forma, estos dos sistemas de diferente naturaleza, el tecnológico y el social, se imbrican formando un sistema emergente denominado *Ciberespacio*.

La tecnología es la que establece el repertorio estructural de lo posible social. Dentro del abanico de lo posible, como estructura límite, es en el segundo nivel donde la contingencia del sistema se actualiza a través de las decisiones constructivas de los usuarios que utilizan las posibilidades tecnológicas para realizar sus necesidades sociales.

Esta interacción entre los dos sistemas o, mejor, subsistemas del Ciberespacio es determinante, ya que su evolución se produce mediante la ampliación de las posibilidades estructurales de los límites tecnológicos.

La tecnología es el límite, pero sus límites son ampliados por la actuación de los agentes sociales.

Si los sistemas en su conjunto están orientados hacia metas, que son las que determinan su evolución o cambios de estado, en el Ciberespacio estos objetivos generales son, desde nuestra perspectiva, la fusión entre los deseos sociales y las posibilidades tecnológicas de su realización.

Es decir, el Ciberespacio evoluciona hacia metas básicamente sociales. Estas metas u objetivos, se cumplen gracias a un proceso permanente en el que son los propios elementos integrantes del sistema los que producen los nuevos elementos del sistema.

I.7 Estructura física del Sistema

Los denominados sistemas de Tecnologías de Información y Comunicaciones (TIC) y sus infraestructuras asociadas (computadoras, programas informáticos y redes) conforman el conjunto de recursos necesarios para encontrar, manipular, convertir, almacenar, administrar, y transmitir la información; constituyéndose en la arquitectura material del

Ciberespacio.

Las TIC son tecnologías para propósitos generales y abarcan desde la infraestructura básica de transporte de datos, los servicios prestados por los operadores a los usuarios finales, las aplicaciones y contenidos en distintos ámbitos, el equipamiento necesario para acceder a dichos servicios y aplicaciones, y la generación de capacidades que estimulen y permitan el uso efectivo por parte de personas y organizaciones.

Una posible clasificación de la estructura de las TIC pueden ser la que distingue entre las redes; las terminales; y los servicios.

Las redes: Telefonía fija; Banda ancha; Telefonía móvil; Redes de televisión; Redes Institucionales; Redes comerciales; y Redes en el hogar.

Las terminales: Teléfonos, Computadoras; Teléfonos móviles; Televisores; Reproductores portátiles de audio y vídeo; Navegador de Internet; Sistemas operativos para computadoras.

Los servicios: Correo electrónico; Búsqueda de información; Banca online; Audio y música; TV y cine; Comercio electrónico; E-administración- E-gobierno; E-sanidad; Educación; Videojuegos; Servicios móviles; Servicios Peer to Peer (P2P); Blogs; Comunidades virtuales.

Respecto a la transmisión de la información, se puede realizar a través de medios de cable y/o inalámbricos. Estos últimos, hacen uso del espectro electromagnético. Las características de los medios de comunicación son la velocidad, la dirección, y el modo de transmisión.[16]

Respecto a las redes de computadoras, *"…permite a los usuarios utilizar un amplio conjunto de aplicaciones…" ya que "…la red no está construida para un único tipo de servicio de comunicaciones, ni siquiera para un grupo reducido de servicios con características similares, sino más bien como una infraestructura genérica sobre la que puedan coexistir las aplicaciones telemáticas actuales y cualesquiera otras por desarrollar."*[17]

La red por excelencia es Internet ya que es una red de redes. Está organizada como una amplia colección de redes autónomas interconectadas. Es una red mundial de equipos digitales conectados mediante diferentes tipos de enlaces (satelitales, por radio, o

[16] Guillermo Adolfo Cuéllar Mejía. Redes y Telecomunicaciones Componentes y Funciones de un Sistema de Telecomunicaciones. Universidad del Cauca. Colombia.
[17] Universidad Politécnica de Madrid (UPM). Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/rst.pdf

submarinos). Estos equipos son, mayoritariamente, computadoras pero incluye, a cualquier artefacto capaz de producir, transmitir y procesar mensajes en forma digital, a condición de que lo haga conforme a un formato previamente convenido y de que pueda hacer llegar estos mensajes, de alguna manera, hasta un router.[18]

Cada una de las subredes constituyentes de Internet global, son en sí mismas, una red de computadoras compuesta por un conjunto arbitrario de enlaces y nodos de comunicaciones. En el nivel más bajo de la jerarquía organizativa de redes que se integran en redes progresivamente más extensas estarían las distintas redes de acceso en las que se ubican los equipos de los usuarios.

Internet es una red con estructura débilmente jerárquica, lo que significa que las estaciones situadas en las subredes periféricas logran comunicarse con el resto a través de un conjunto de redes troncales de interconexión que constituyen el primer nivel.

Otra característica estructural del actual Internet es que las múltiples subredes de la máxima responsabilidad (o cobertura) jerárquica, pertenecen y están administradas por organizaciones diferentes, tanto públicas como privadas.

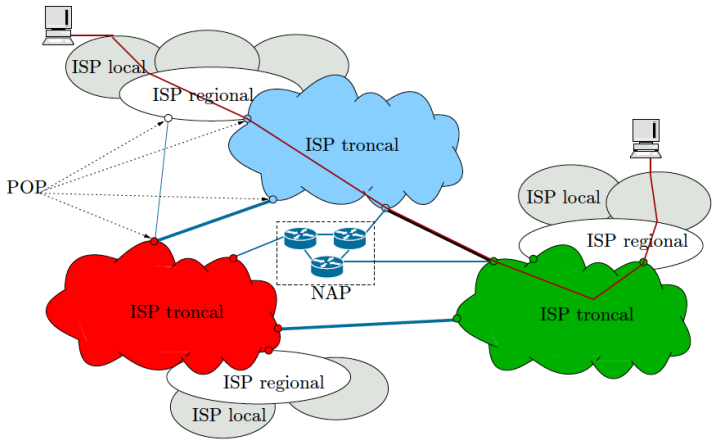


Figura 1.1

Estructura de Internet, con sus tres niveles de operaciones:
redes de acceso (servicio local), redes de segundo nivel (servicio regional/nacional) y
redes troncales (servicio nacional/internacional)

Fuente: GTIC

Todas las troncales suelen tener conexión directa entre sí, lo que significa que operan como pares en una relación mutua de dos a dos, y prestan sus servicios de transporte de tráfico a diferentes subredes de menor tamaño, de ámbito continental, nacional o regional,

[18] Universidad Politécnica de Madrid (UPM). Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/rst.pdf

que actúan, por tanto, como clientes de las de primer nivel. Habitualmente, las redes subsidiarias disponen de conexión con varias de las subredes troncales, ya sea por razones de redundancia, o bien por motivos de ingeniería de tráfico.

En el segundo nivel se ubican las redes de los diferentes proveedores de servicios de Internet (ISPs). En la red de un ISP, aquellos routers que sirven para conectarse a otros ISPs, en el mismo o en distinto nivel de la jerarquía, se suelen denominar puntos de presencia (POP, por su siglas en inglés Point of Presence).

Un POP es, físicamente, un grupo de conmutadores de paquetes de alta velocidad en el que terminan enlaces procedentes de otros ISPs. El intercambio de tráfico entre ISPs diferentes suele depender de acuerdos puntuales de carácter contractual privado.

Sin embargo, para garantizar a los usuarios finales la imparcialidad en el reparto de tráfico por las diferentes troncales, existen los denominados puntos neutros, puntos de acceso de red NAP (Network Access Point).

Un punto neutro se construye físicamente igual que un POP, disponiendo en paralelo suficientes conmutadores, pero suele estar gestionado por un tercero y ofrece sus servicios de intercambio de tráfico a todos los ISPs en igualdad de condiciones.

Un NAP usualmente pertenece a una operadora importante de telecomunicaciones, a una gran compañía proveedora de servicios de acceso a Internet, o a algún consorcio de varias empresas del sector, como es el caso de CABASE,[19] el punto neutro argentino.

En el tercer nivel aparecen las redes de acceso, aquellas más próximas a los usuarios y que soportan directamente los sistemas finales. Las redes de acceso son comúnmente parte de alguna red de segundo nivel o bien pertenecen a algún proveedor de servicios local. En todo caso, mantienen una relación uno a uno con ellas, es decir, es una única red de segundo nivel la que les da acceso al resto de Internet. Suelen tener, además, topologías simples: redes de acceso múltiple en forma de bus o estrella, o enlaces punto a punto terminados en un equipo concentrador de líneas como en un acceso residencial ADSL.

[19] Cámara Argentina de Internet. Disponible en http://www.cabase.org.ar consultado el 30-SEP-12.

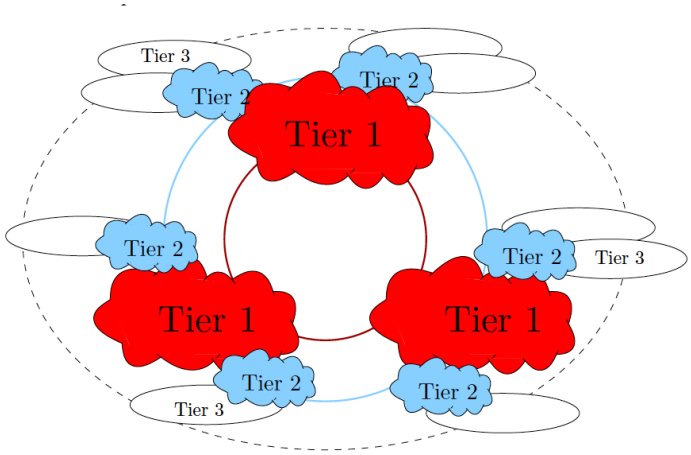


Figura 1.2

Jerarquía de redes y proveedores de servicio en Internet
Un Tier es un ISP

Fuente: GTIC

Para resumir, una gran red de computadoras con una estructura notoriamente compleja formada a partir de la imbricación de múltiples redes troncales, miles de redes de segundo nivel y cientos de miles de subredes capilares de acceso en las que residen los usuarios finales.

Cada una de estas subredes puede estar construida con tecnologías dispares y dar servicio a pocos o muchos usuarios, pero todas comparten los mismos principios básicos de funcionamiento y un protocolo común que les permite entenderse. La administración y el control de operaciones de la red es completamente descentralizado y autónomo, como lo es también la organización topológica de cada una de las redes componentes y de la misma superestructura. Así, existen múltiples troncales en Internet que operan en paralelo, cada una soportando decenas de redes de segundo nivel que, no obstante, además de la relación jerárquica que mantienen con las troncales suelen estar también interconectadas directamente entre sí. Las redes de segundo nivel engloban (o prestan servicio) a otras redes de ámbito más restringido y así sucesivamente.

En Internet el protocolo común a todos los sistemas finales y conmutadores, que en último término, es el lenguaje universal que garantiza que el sistema global funcione, se llama Internet Protocol (IP) y se encarga fundamentalmente de definir un formato común a todos los paquetes que la red transporta, además de establecer la forma e interpretación de las direcciones.

La comunicación entre computadoras en una red se logra a través de un lenguaje preciso, que debe asegurar que todos los equipos lo comprendan, para poder identificarse entre si. Esto último es la esencia de Internet: todos los equipos deben tener una

dirección IP, un identificador único, que toma la forma de una serie de cuatro (IPv4) a ocho (IPv6) grupos de cuatro números cada grupo separados por puntos. Lo necesario es que las direcciones sean únicas: es imposible conectarse a un sitio web con un navegador si la dirección IP reenvía a docenas de computadoras en cualquier lugar del mundo. Por lo tanto, es importante no asignar direcciones IP de cualquier modo.

Por esta razón, es la Corporación para la Asignación de Nombres y Números de Internet (ICANN por sus siglas en inglés) quien, en primer lugar, determina qué rangos de direcciones IP están disponibles en el mundo y quién tiene el derecho de utilizarlos. A nivel local, son las organizaciones llamadas RIR (Regional Internet Register) las que distribuyen las direcciones IP que la ICANN les ha asignado. Hay cinco RIR en el mundo.

Sin embargo, la dirección numérica IP, que es vital para que las computadoras se reconozcan, no es muy práctica para los usuarios. Por eso existen también las direcciones de texto, que son las que utilizamos todos los días, como por ejemplo www.minidef.gov.ar. Cada dirección expone toda la información necesaria para saber a qué país pertenece (lo sabemos a través del último segmento, la extensión: ".ar" significa Argentina), o si se trata de un sitio gubernamental (.gov) o comercial (.com).

Las direcciones de texto son una decisión práctica, pero para que funcionen, es necesario traducir a las computadoras, en cada conexión, la dirección en clave IP.

Para esto intervienen los Servidores de Nombres de Dominio (DNS por su sigla en inglés Domain Name System).

Cuando escribimos cualquier dirección en un navegador web, como www.minidef.gov.ar por ejemplo, se hace un primer pedido al Servidor de Nombre de dominio, que indica los servidores que pueden proporcionar una respuesta para el dominio.gov. Uno de esos servidores determinará qué otro servidor es capaz de dirigir a la zona de minidef.gov. Y este último servidor podrá aportar la dirección IP completa del sitio buscado. Esta secuencia de consulta se realiza en cada visita al sitio. Los servidores capaces de realizar el primero paso, es decir, dirigir hacia los servidores que administran los dominios llamados de primer nivel (.com, .org, .gov, .net), se llaman servidores raíz de DNS. Hay sólo trece en todo el mundo.

Cada uno de estos servidores tienen muchos "espejos", y en ocasiones ni siquiera están alojados en un solo lugar. En total, estos trece servidores, absolutamente vitales para el funcionamiento de Internet, se distribuyen en todo el mundo en casi 170 ciudades. Y aunque cada día sean supervisados por empresas privadas, universidades o el gobierno, siempre intervienen delegaciones de ICANN, que en última instancia, toma todas las

decisiones.

Hay una gran cantidad de organizaciones que participan en la regulación de Internet y en el establecimiento de estándares: W3C, Internet Society (ISOC), Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), y otras. Pero en última instancia, el funcionamiento de Internet depende principalmente de ICANN, quien a su vez depende del Departamento de Comercio estadounidense, que designa a todos sus miembros.

Para un mayor detalle de todas las organizaciones que intervienen, a lo que se denomina Ecosistema de Internet, ver el Anexo A.

CAPÍTULO II. EL CIBERESPACIO EN ARGENTINA

En el capítulo anterior pudimos apreciar que el Ciberespacio es un sistema emergente de la imbricación de dos sistemas de diferente naturaleza, el social y el tecnológico, y las posibilidades emergentes del primero están en función de los desarrollos que se dan en el segundo.

Ambos sistemas presentan condiciones de desarrollo dispares en las distintas unidades de análisis a donde se lleve el foco de atención, sean estas unidades, políticas, económicas, sociales, militares, etc.

En relación a las redes de computadoras, uno de los componentes estructurales de las TIC, el Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) expresa: *"Una red de ordenadores exhibe una organización interna tan compleja y una pauta de evolución tan dinámica como la de la sociedad a la que sirve; en definitiva, como la de cualquier organismo viviente."*[20]

Así, y a pesar de que el Ciberespacio se constituye como un sistema global, entendemos que en la Republica Argentina el Ciberespacio posee algunas características propias y particulares.

II.1 Estructura física del Sistema en Argentina

En la Republica Argentina, la infraestructura de las TIC responde a la misma lógica de funcionamiento que la descripta en el capítulo anterior, y se encuentra interconectada mediante diferentes tipos de enlaces (satelitales, por radio, o submarinos). Ver Anexo B.

El ecosistema de las TIC abarca desde la infraestructura básica de transporte de datos, los servicios prestados por los operadores a los usuarios finales, las aplicaciones y contenidos en distintos ámbitos (entretenimiento, educación, gobierno, comercio, etc.), el equipamiento necesario para acceder a dichos servicios y aplicaciones, y por último la generación de capacidades que estimulen y permitan el uso efectivo por parte de personas y organizaciones.[21]

Respecto a la red de fibra óptica, se encuentra en Buenos Aries el primer NAP

[20] Universidad Politécnica de Madrid (UPM). Grupo de Tecnologías de la Información y las Comunicaciones (GTIC) http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaRst/rst.pdf

[21] Comisión de Planificación y Coordinación Estratégica 2010. Plan Nacional de Telecomunicaciones "Argentina Conectada".

Nacional, administrado por CABASE, y se constituye como el punto de intercambio de tráfico nacional de Internet. Asimismo, cuenta con NAP regionales en Buenos Aires, Rosario, Neuquén, Bahía Blanca, Mendoza, Santa Fe, La Costa, Córdoba y La Plata, y prevé la inauguración de otros en Mar del Plata, San Luís, Paraná, Resistencia, Corrientes, Bariloche y Posadas. Ver figura 2.1.

El NAP nacional esta conectado a la RIR LACNIC (por su sigla en inglés Latin America and some Caribbean Islands). Ver Anexo C.

Por otra parte, si bien hay múltiples ISPs gran parte de la infraestructura es propiedad de las empresas Telecom S.A. y Telefónica S.A., así como también, gran parte de las redes de última milla.[22]

Actualmente, esta en ejecución el Plan Nacional de Telecomunicaciones "Argentina Conectada" cuya finalidad es la de articular el desarrollo de las TIC en la República Argentina. El mismo, tiene como ejes estratégicos: la inclusión digital; la optimización del uso del espectro radioeléctrico; el desarrollo del servicio universal; la producción nacional y generación de empleo en el sector de las telecomunicaciones; la capacitación e investigación en tecnologías de las comunicaciones; la infraestructura y conectividad; y el fomento a la competencia. El plan de acción, definió las estrategias y acciones específicas para alcanzar los objetivos dispuestos por el Poder Ejecutivo Nacional, estando previsto que sea desarrollado entre los años 2010 y 2015, y revisado en función de sus impactos y necesidades de adecuación. [23]

Cabe destacar, que dentro de la Comisión de Planificación y Coordinación Estratégica 2010 no fue incluido ningún organismo del Ministerio de Defensa.

[22] Diario Pagina 12. http://www.pagina12.com.ar/diario/suplementos/cash/17-6304-2012-09-30.html
[23] Comisión de Planificación y Coordinación Estratégica 2010. Plan Nacional de Telecomunicaciones "Argentina Conectada".

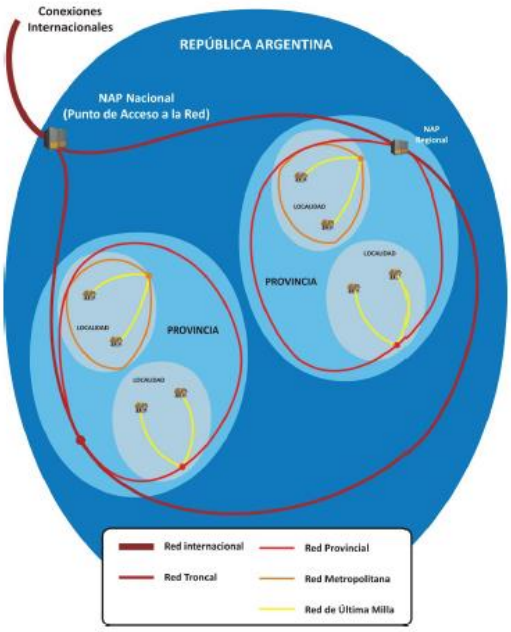


Figura 2.1

Representación esquemática de Red Federal de Fibra Óptica

Fuente: Plan Nacional de Telecomunicaciones "Argentina Conectada".

II.2 Actores

Si tenemos en cuenta la definición adoptada del termino Ciberespacio, y definiendo al termino Actores, como todo sujeto que dirige sus acciones en pos de un fin determinado; estamos en condiciones de aceptar que toda persona que tenga acceso a cualquier tipo de equipo digital conectado a una red, y que posea los suficientes conocimientos como para ejecutar acciones, podría ser considerado un actor que interactúa en el Ciberespacio.

Ahora bien, para los objetivos perseguidos en el presente estudio, nos resulta necesario tomar, aunque arbitrariamente, una clasificación de actores relevantes.

Al igual que en gran parte del mundo, en la Republica Argentina, los actores relacionados con las TIC son de los mas diversos tipos: organismos estatales, grandes empresas multinacionales, universidades, fundaciones, cooperativas, cámaras empresariales, y PYMES, entre otras.

Desde el punto de vista regulatorio, las principales autoridades locales son: la Dirección Nacional del Registro de Dominios de Internet (NIC argentina, por sus siglas en inglés Network Information Center), la Red de Interconexión Universitaria (ARIU), y la Comisión Nacional de Comunicaciones (CNC).

La NIC Argentina tiene como responsabilidad primaria entender en la

administración del Dominio de Nivel Superior Argentina (.AR) y en el registro de nombres de dominio de Internet de las personas físicas y jurídicas.[24]

La ARIU es la entidad en la que NIC Argentina delegó la responsabilidad de la operación estable y confiable de la base de datos autorizada, llamada Sistema de Nombres de Dominios "edu.ar". Es el DNS que indexa todos los dominios "edu.ar" con los números IP.[25]

Concretamente, a la ARIU le atañe proveer las informaciones de lugar, relacionadas con los nombres de dominios registrados bajo ".edu.ar". Además, suplir las facilidades necesarias para agilizar el proceso de registro, modificación y actualización. La ARIU facilita el registro de su dominio en forma gratuita a todas las entidades educativas de la República Argentina.

La CNC es un organismo descentralizado que funciona en el ámbito de la Secretaría de Comunicaciones del Ministerio de Planificación Federal, Inversión Pública y Servicios, cuya misión y funciones son la regulación, contralor, fiscalización y verificación de los aspectos vinculados a la prestación de los servicios de telecomunicaciones, postales y de uso del Espectro Radioeléctrico.

En tal sentido, el Organismo tiene la facultad de administrar, gestionar, monitorear y controlar los servicios y sistemas de telecomunicaciones entre los que se encuentran los de telefonía, Internet, audio texto, satélites, servicios de comunicaciones marítimos y aeronáuticos entre otros, así como intervenir en el cumplimiento de las condiciones, estándares de calidad y demás obligaciones vinculados a la prestación del Servicio Postal Básico Universal, prestadores privados y/u otros servicios que se consideren obligatorios del Correo Oficial.[26]

Desde el punto de vista de la infraestructura, encontramos a la Comisión de Planificación y Coordinación Estratégica 2010; y a las empresas de Telecomunicaciones (TELCOs) Telecom Argentina S.A. y Telefónica de Argentina S.A.

Desde el punto de vista de la seguridad, se encuentra a la Oficina Nacional de Tecnologías de Información (ONTI) de la Secretaria de Gestión Pública; el Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad; y los tres Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT por su sigla en Inglés), que son el dependiente de la Universidad Nacional de La Plata, el de la Red de Cajeros Automáticos BANELCO; y el de CABASE.

[24] Presidencia de la Nación. Decreto 189/2011.
[25] Dirección Nacional del Registro de Dominios de Internet. www.nic.ar
[26] Comisión Nacional de Telecomunicaciones. http://www.cnc.gov.ar/institucional/nuestro_org_introduccion.asp

La ONTI tiene como principal objetivo dar respuesta a los incidentes en redes, centralizando y coordinando los esfuerzos para el manejo de los incidentes de seguridad, que afecten los recursos informáticos de la Administración Pública Nacional; es decir, cualquier ataque o intento de penetración a través de sus redes de información.

El Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 y sus modificatorios, los organismos interjurisdiccionales, y las organizaciones civiles y del sector privado que así lo requieran, así como al fomento de la cooperación y colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías.[27]

Los Centros de Respuesta a Incidentes de Seguridad Informática son equipos, reconocidos por la Dirección de su organización, como responsables de gestionar los incidentes de seguridad informática que le competan según su alcance y comunidad.

Estos grupos deben ser capaces de brindar información oportuna sobre cómo responder a los distintos tipos de incidentes, determinar su impacto, alcance y naturaleza, comprender las causas técnicas, investigar soluciones, realizar recomendaciones, coordinar y dar apoyo para la implementación de las estrategias de respuesta con las partes involucradas, difundir información sobre los tipos de incidentes más frecuentes y toda información relevante que permita estar preparado para dar respuesta a los mismos y mitigar sus efectos, coordinar y colaborar con otros actores, tales como proveedores de Internet (ISP), otros grupos de seguridad, etc.

En lo que respecta al Ciberespacio y a su uso en la defensa, *"…su dominio no sólo resulta esencial para el ejercicio del comando y control, y para el funcionamiento en red del sistema, sino también para repeler y conjurar amenazas militares estatales externas que puedan producirse utilizando al llamado Ciberespacio como vía de ejecución o teniéndolo como objetivo. Para ello el desarrollo de un núcleo orgánico-funcional, con una doctrina específica, es un desafío para el futuro del sistema de defensa."*[28]

[27] Jefatura de Gabinete de Ministros. Resolución 580/2011.
[28] Libro Blanco de la Defensa 2010.

El desafío de establecer el núcleo orgánico-funcional con una doctrina específica, esta siendo desarrollado actualmente en el Estado Mayor Conjunto de las Fuerzas Armadas.

II.3 Ciberespacio. Nuevo ámbito de lucha

La misión principal de las Fuerzas Armadas, Instrumento Militar de la Defensa Nacional (IMDN), es la de conjurar y repeler toda agresión externa militar estatal, a fin de garantizar y salvaguardar de modo permanente los intereses vitales de la Nación, cuales son los de su soberanía, independencia y autodeterminación, su integridad territorial y la vida y libertad de sus habitantes.[29]

El Ciberespacio *es espacio y es medio,*[30]que se constituye en nuevo ámbito de lucha. Este nuevo ámbito requiere entonces, el desarrollo de capacidades, asignación de fuerzas, misión, organización y funciones específicas para contribuir al logro de la misión del IMDN.

En este sentido, en el Libro Blanco de la Defensa 2010 *"se considera estratégico avanzar en la investigación, desarrollo y aplicación de las tecnologías aeroespaciales, nucleares y aquellas vinculadas al Ciberespacio desde el Sistema de Defensa Nacional, en el marco de lo establecido en la Constitución Nacional y los múltiples acuerdos vigentes de los cuales el país es signatario."*

Un aspecto importante para destacar, es que en el siglo XXI los ámbitos terrestre, marítimo, y aeroespacial, interactúan en forma sinérgica con el Ciberespacio, y al mismo tiempo, y cada vez mas, las acciones que se efectúan en cada uno de ellos, se vuelven dependiente de el.

Al respecto, y específicamente en relación con las operaciones militares, encontramos nuevamente en el Libro Blanco de la Defensa 2010 que *"Las tecnologías aeroespaciales y ciberespaciales constituyen contribuciones críticas para hacer viables los efectos pretendidos en el marco de una estrategia de carácter defensivo. Éstas son consideradas esenciales para contar con una alerta estratégica temprana frente a una eventual agresión militar estatal externa, y para desarrollar eficazmente la conducción de las operaciones militares y repeler con éxito dicha agresión. Asimismo, estas tecnologías contribuyen al control efectivo de los espacios terrestres, marítimos y aeroespaciales de la*

[29] Decreto 1714 / 2009 Directiva de Política de Defensa Nacional.
[30] Joaquín Mª Aguirre Romero 2004. Espéculo. Revista de estudios literarios. Universidad Complutense de Madrid. http://www.ucm.es/info/especulo/numero27/cibercom.html

Nación."

La formación de cibercombatientes resulta un imperativo improrrogable. El grado de especificidad técnica del ambiente operacional y las potencialidades de las armas que tendrán a disposición, requerirá de fuerzas especialmente instruidas y adiestradas.

No es una novedad, que la calidad de los combatientes y los avances tecnológicos del armamento que dispongan, son factores claves para el éxito en el combate.

Pero en el Ciberespacio, encontramos que la idoneidad, los conocimientos y la experiencia de los cibercombatientes, son un factor determinante y que predomina sobre el nivel tecnológico del armamento con que se enfrentan los contendientes.

El preeminente carácter social del Ciberespacio, obligara a que las operaciones ciberespaciales deban ser ejecutadas por equipos interdisciplinarios integrados por, al menos, cibercombatientes, sociólogos, filósofos, abogados, psicólogos, y especialistas en comunicación social, entre otros.

Por otra parte, el Ciberespacio como ámbito de lucha presenta dos grandes ventajas respecto a otros ámbitos, y son la libre disponibilidad en el mercado y el bajo costo del equipamiento necesario para afrontar las operaciones.

II.4 Marco Legal

A través de las leyes 23554 de Defensa Nacional y 24059 de Seguridad Interior, y el Decreto 727/2006 que reglamentó la Ley de Defensa Nacional, la República Argentina consagró la diferenciación conceptual entre Defensa Nacional y Seguridad Interior, estableciendo los objetos a los que están enfocados cada uno de los sistemas.

El de defensa, a conjurar agresiones de origen externo perpetradas por fuerzas armadas pertenecientes a otro u otros Estados[31]; en tanto el de la Seguridad Interior se enfoca a la prevención y persecución de delitos contenidos en el Código Penal y otras leyes especiales.[32]

Esta diferencia en los fenómenos a atender implica adiestramientos, equipamientos y doctrinas de empleo específicas.

Sin embargo, las singulares características del Ciberespacio y las acciones que se pueden ejecutar en y a través del mismo, hacen que esta diferenciación taxativa entre Defensa Nacional y Seguridad Interior, que se ha llevado a la práctica en los ámbitos terrestre,

[31] Decreto 727/2006 Reglamentación de la Ley Nº 23554.
[32] Decreto 1273/92 Reglamentación de la Ley Nº 24059.

naval, y aeroespacial no sea de aplicación útil en el ámbito ciberespacial.

Basta con mencionar que el Ciberespacio, entre otras posibilidades, brinda la oportunidad de efectuar ataques en total anonimato y con escasas probabilidades de identificar al agresor, atacar desde un lugar remoto del planeta sin quedar sujeto a ningún tipo de jurisdicción territorial y/o legal; gradar el daño a efectuar desde una incidencia marginal a una catastrófica, posibilidad de retardar la acción destructiva y activarla remotamente y/o de manera autónoma; provocar daños inmateriales con efectos materiales indirectos de difícil determinación y mensura; y por si fuera poco, todo esto se puede llevar a cabo en fracción de segundos.

De cualquier manera, esta cuestión no es objeto de análisis del presente estudio, aunque se hace necesaria su mención al los efectos de contextualizar las normativas legales vigentes con este nuevo ambiente operacional.

Hasta ahora, la *ciberguerra*, tal como se la definió en el capítulo I, es el único caso en donde sería de aplicación el concepto de agresión establecido por la resolución 3314 de la Organización de las Naciones Unidas (ONU), el que fue retenido como tal por el Decreto 727/2006 reglamentario de la Ley Nº 23554 de Defensa Nacional.

II.4.1 El Derecho Internacional Humanitario (DIH) y la guerra cibernética

Si bien no existe disposición alguna en ningún instrumento de DIH que reglamente directamente la ciberguerra, las normas prescriptivas existentes de derecho humanitario son suficientes para conservar la protección de que gozan las personas civiles, los bienes de carácter civil y otras personas jurídicas contra los efectos de las hostilidades.

A través de sus normas generales, el DIH regula todos los medios y métodos de guerra, incluido el uso de todas las armas. En particular, el artículo 36 del Protocolo adicional I a los Convenios de Ginebra demuestra que las disposiciones generales del DIH se aplican a las nuevas tecnologías.

De manera general, se puede afirmar que *"...si los medios y métodos de la guerra cibernética producen los mismos efectos en el mundo real que las armas convencionales (destrucción, desorden, daños, lesiones o muerte), se rigen por las mismas normas que las armas convencionales."* [33]

Sin embargo, es importante resaltar que *"el derecho internacional humanitario*

[33] Cordula Droege, asesora legal del CICR. No hay lagunas jurídicas en el ciberespacio Entrevista 16-08-2011 http://www.icrc.org/spa/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

o DIH sólo entra en juego si las operaciones cibernéticas se cometen en el contexto de un conflicto armado, sea entre Estados, entre Estados y grupos armados organizados, o entre grupos armados organizados." Por ende, "…en situaciones de conflicto armado, el DIH se aplica cuando las partes recurren a medios y métodos de guerra basados en operaciones cibernéticas."[34]

Ahora bien, ha quedado claro que no existe vacío legal alguno en el DIH respecto a la ciberguerra, sin embargo se plantean algunas dificultades sobre su pertinencia y forma de aplicación en la práctica, ya que las normas del DIH se relacionan con los principios de distinción, de proporcionalidad y de precaución.[35]

Una de estas dificultades es el anonimato de las comunicaciones, y por ende, en el Ciberespacio, muchas veces, es casi imposible rastrear a quien está detrás de una operación cibernética.

Puesto que todas las leyes se basan en la atribución de responsabilidad, y en el DIH, la responsabilidad se atribuye a una parte en un conflicto o a un individuo, si no es posible identificar al autor de una operación determinada ni, por ende, el vínculo de la operación con un conflicto armado, resulta extremadamente difícil determinar si el DIH es aplicable a la operación.

Otra dificultad para la aplicación de las normas del DIH es la interconectividad entre los sistemas informáticos civiles y militares.

Este aspecto, dificulta fundamentalmente la distinción entre objetivos militares y bienes de carácter civil; la determinación de proporcionalidad en los ataques; y la justificación de la ventaja militar que los ataques puedan acarrear.

Así pues, aunque el derecho humanitario, en su forma actual, es suficiente para salvaguardar, en general, a aquellos que se propone proteger de los efectos de los ataques a través de redes informáticas, siguen existiendo significativas imperfecciones prescriptivas.[36]

II.5 Operaciones militares en el Ciberespacio

Como se mencionara en el capítulo I, en el Ciberespacio, es posible realizar ciertas acciones que lo acercan más a una nueva forma de realidad, que a una nueva forma de ficcionalidad.

---

[34] Ídem.
[35] Ídem.
[36] Schmitt, Michael: La guerra de la información: los ataques por vía informática y el jus in bello, Comité Internacional de la Cruz Roja, 2002, en: http://www.icrc.org/spa/resources/documents/misc/5tecg3.htm

En efecto, las acciones que pueden realizarse en esta nueva forma de realidad, pueden ser potenciadoras del desarrollo socioeconómico de un país, pero también pueden ser amenazas para sus intereses vitales.

Una característica diferenciadora de las operaciones ciberespaciales o cibernéticas, es la cualidad no cinética del armamento a ser empleado. Ya no son necesarios costosos misiles o bombas inteligentes para provocarle daños reales a un adversario. Basta con reunir un hombre con conocimiento, una computadora conectada a Internet, y algunas instrucciones digitales, para provocar daños no solo en el mundo virtual, sino también, en el mundo real.

Como ya se ha mencionado, no hay acuerdo en la definición del término Ciberespacio, y por ende, tampoco lo hay para definir que son las operaciones ciberespaciales o cibernéticas.

Así, por ejemplo, los estadounidenses las definen como *"el empleo de capacidades ciberespaciales donde el objetivo primario es el de alcanzar objetivos militares o efectos en o por el Ciberespacio."*[37]

Droege (2011) emplea el término "operaciones cibernéticas" para referirse *"…a las operaciones realizadas contra un ordenador, o mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos."*[38]

En función de que la legislación vigente en la Republica Argentina separa la esfera de la Defensa de la de Seguridad, se hace necesario adecuar la definición del término "operaciones ciberespaciales" como el *empleo de capacidades ciberespaciales para alcanzar objetivos militares a través o en el Ciberespacio*.

Como se expresara anteriormente, en el Ciberespacio se establecen simultáneamente tres tipos de intercambios de información que forman un solo proceso. Sin embargo, cada uno de estos tipos de intercambio son de distinta naturaleza, tienen fines y condicionantes distintos.

En este sentido, a las operaciones ciberespaciales se las puede clasificar siguiendo la citada distinción de los tipos de intercambio de información. Así, tendríamos operaciones ciberespaciales, tendientes a afectar o resguardar, las relaciones de intercambio de información entre hombres y máquinas, máquinas y máquinas, hombres y hombres.

---

[37] United States Air Force Doctrine Document 3-12 15 July 2010. Ciberspace Operations. Traducción efectuada por el autor del presente trabajo.

[38] Cordula Droege, asesora legal del CICR. No hay lagunas jurídicas en el ciberespacio Entrevista 16-08-2011 http://www.icrc.org/spa/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

A su vez, se las puede clasificar también, en las clásicas categorías de ofensivas o defensivas.

Hasta hoy se afirma que *"cuando se incursiona en el nivel operacional, se descubre que no hay ley ni principio lo suficientemente apto, que permita lidiar con un ambiente tan cambiante e inestable como la guerra. No hay guerra que se parezca a la anterior, dice el axioma empírico. Por tanto, si cada conflicto es único e irrepetible, sería un contrasentido querer aplicar recetas pasadas al futuro.*"[39]

Sin embargo, si hasta hoy la experiencia indicaba que en el nivel operacional debía imperar la unidad de comando y de esfuerzo, en la ciberguerra ese imperativo se magnifica.

El Ciberespacio ya no solo requiere de accionar militar conjunto, sino también de una estrecha relación y accionar interagencial, conformando el diseño de una cadena decisional capaz de dar respuesta a la abrumadora velocidad con que se producen los hechos.

Las operaciones ciberespaciales se ejecutan en milisegundos, y el crucial enlace que proporciona el nivel operacional entre los objetivos estratégicos y el empleo táctico de las fuerzas, requiere de una estructura que no admite dilación alguna.

El mayor desafío para los conductores militares, se presenta en el área del arte operacional.

[39] Manual de Estrategia y Planeamiento para la Acción Militar Conjunta Nivel Operacional – La Campaña. Revisión 2011.

CONCLUSIONES

Creemos que el presente estudio contribuyó a la comprensión del complejo ámbito que constituye el Ciberespacio, al que hemos definido como un "espacio relacional que se construye a través del intercambio de información constituido sobre los sistemas de Tecnologías de Información y Comunicaciones," y nos permite arribar a las siguientes conclusiones.

Nos encontramos frente a la emergencia irrefrenable de un nuevo ámbito de realidad, el Ciberespacio. Ante este hecho, entendemos que la realidad, ha perdido para siempre la exaltada univocidad del término, el cual estaba claramente asociado a la materialidad de las cosas. Ahora es necesario efectuar la distinción "material" o "virtual" del término "realidad".

En relación a los actores que están involucrados en el Ciberespacio en el caso particular de la Republica Argentina, los identificamos en el área de los sistemas de las TIC, encontrando una red conformada por organismos públicos, empresas privadas, y cámaras empresariales, que funciona de manera armónica.

Respecto a las condiciones de producción de las nuevas operaciones militares en el Ciberespacio en la Republica Argentina, encuentran su primera dificultad en el hecho de no contar aún con el núcleo orgánico-funcional necesario; y con una doctrina específica. Se detectan algunos condicionantes de índole legal que acotarían, de manera poco útil, la libertad de acción.

Los conceptos formados a partir y en función de los ámbitos naturales (terrestre, naval, aeroespacial) en los que esta inmersa nuestra cotidianeidad, dificultan la visualización y la comprensión del Ciberespacio como un nuevo ámbito de realidad.

Asimismo, pudo reconocerse que la hipótesis que nos planteamos, ha sido refutada; ya que los desafíos operacionales en el Ciberespacio dentro del ámbito de la República Argentina, ya han comenzado a establecerse, y al mismo tiempo, los actores involucrados perciben como un beneficio la realización de operaciones ciberespaciales. Cabe aclarar, que gran parte de estos actores poseen un concepto, respecto a las operaciones ciberespaciales, más ligado a la seguridad informática que a la defensa de intereses vitales.

El presente trabajo nos permitió identificar algunos de los principales desafíos operacionales, entre los que se encuentran:

- Desarrollar una fuerza de cibercombatientes, con saberes específicos, y con capacitación para el trabajo en equipos interdisciplinarios.

– Establecer, en torno a la conducción de las operaciones ciberespaciales, una estructura decisional eficiente, con una visión dinámica y transversal dentro del Estado, entre Estados y organismos supraestatales.
– Redefinir aspectos relativos al arte operacional.
– Propiciar la investigación y desarrollo de nuevas tecnologías y capacidades ciberespaciales.
– Establecer nuevas estrategias de resguardo de toda infraestructura crítica.

Asimismo, y como prerrequisito para el logro de los desafíos operacionales, consideramos pertinente alcanzar otros desafíos tales como:

– Lograr consensos básicos respecto a la definición de actos de guerra cibernética.
– Adaptar la legislación vigente para que permita encuadrar claramente una agresión que emplee el Ciberespacio, y valorice el derecho del Estado a su legítima defensa.
– Capacitar y concientizar a todos los integrantes del Sistema de Defensa.

Finalmente, creemos que existen oportunidades para investigar aspectos relativos a los beneficios y obstáculos de la separación actual de las áreas de Seguridad y Defensa; y el perfil de los recursos humanos necesarios para ejecutar las operaciones ciberespaciales; entre otros.

De cuanto se logre avanzar en los aspectos relativos al Ciberespacio, así será la magnitud de "*…la consolidación definitiva de unas Fuerzas Armadas modernas, adiestradas y alistadas para enfrentar los desafíos que el futuro le depare a nuestro país…"*[40]

[40] Ministro de Defensa de la Republica Argentina. 2010. Citado en el Libro Blanco de la Defensa 2010.

Bibliografía

Libros:

CARR, Jeffrey. 2011. Inside Cyber Warfare: Mapping the Cyber Underworld. Second Edition. s.l. O´Reilly.

CLARKE, Richard A.; KNAKE, Robert K. 2010. Cyber War: The Next Threat to National Security and What to Do About It. New York. Harpers-Collins Publishers.

GIBSON, William. 2001. Neuromante. Barcelona. Ediciones Minotauro.

KUEHL, Dan. 2009. From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management. Estados Unidos. College-National Defense University.

LUHMANN, Niklas. 1998. Sistemas sociales. Lineamientos para una teoría general. Barcelona, Anthropos.

SIBILIA, Paula. 2005. El Hombre Postorgánico: Cuerpo, subjetividad y tecnologías digitales. Buenos Aires. Fondo de Cultura Económica.

RAIN, Ottis y LORENTS, Peeter. 2010. Cyberspace: Definitions and Implications. Estonia. Cooperative Cyber Defence Centre of Excellence.

TOFFLER, A. y TOFFLER, H. 1993. War and AntiWar: Survival at the Dawn of the 21 st Century. Boston. Little Brown and Co.

Manuales:

DOD Dictionary of Military and Associated Terms. Joint Doctrine Division, J-7, Joint Staff. Disponible en: http://www.dtic.mil/doctrine/jel/doddict/ Página en inglés. Fecha de captura: 07/06/12.

UNITED STATES AIR FORCE. Cyberspace Operations. Air Force Doctrine Document 3-12. 2011. Disponible en: http://www.google.com.ar/url?sa=t&rct=j&q=air%20force%20doctrine%20document%203-12&source=web&cd=1&ved=0CFQQFjAA&url=http%3A%2F%2Fwww.e-publishing.af.mil%2Fshared%2Fmedia%2Fepubs%2Fafdd3-12.pdf&ei=_AL6T9auDYr10gHugo3dBg&usg=AFQjCNGn3BZbA35YRbehfYiHpiAzidHTmw&cad=rja Página en inglés. Fecha de captura: 07/06/12.

UNITED STATES OF AMERICA. 2011. Department of Defense. "Strategy for Operating in Cyberspace". Disponible en: http://www.google.com.ar/url?sa=t&rct=j&q=dod%20strategy%20for%20operating%20in%20cyberspace%20july%202011&source=web&cd=1&ved=0CEgQFjAA&url=http%3A%2F%2Fwww.defense.gov%2Fnews%2Fd20110714cyber.pdf&ei=fQP6T8iRFIKi8QSkzeD9Bg&usg=AFQjCNHvrT6jxVqzz1IXyKcTrM3Al6t_Cw&cad=rja Página en inglés. Fecha de captura: 07/06/12.

Periódicos:

KABAY, M.E. 1995. Prepare yourself for information warfare. Computer World. v. 29, no. 12, p. S2. Disponible en: http://www.computerworld.com/search/AT-html/9503/950301SL9503lead.asc.html Página en inglés. Fecha de captura: 07/06/12.

Artículos:

AGUIRRE ROMERO, Joaquín María. 2004. Espéculo. Revista de estudios literarios. Universidad Complutense de Madrid. http://www.ucm.es/info/especulo/numero27/cibercom.html Página en castellano. Fecha de captura: 01/07/12

BOYLE, James. 1997. Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors. Durham. Disponible en: scholarship.law.duke.edu/.../viewcontent.cgi?... Página en inglés. Fecha de captura: 12/06/12.

LIBICKI, Martin C. 2009. Cyberdeterrence and cyberwar. Santa Mónica. RAND Corp. Disponible en: www.rand.org/pubs/monographs/2009/RAND_MG877.pdf Página en inglés. Fecha de captura: 07/06/12.

SHORT, Carolina. Cambios en el paradigma de los objetos desde la era industrial a la era de la información. s.l. Disponible en: http://bigital.com/castellano/files/2010/06/Carolina_Short-diseno-era-de-la-informacion.pdf Página en castellano. Fecha de captura: 01/07/12.

STEIN, G.J. Information War–Cyberwar–Netwar. Battlefield of the Future. 21st Century Warfare Issues. Disponible en: http://www.cdsar.af.mil/battle/chp6.html Página en inglés. Fecha de captura: 07/06/12.

Otros documentos:

ALATORRE CUEVAS, Israel. Neuromante: el futuro que llegó. Número 25 de la revista: "Tramas, Subjetividad y Procesos Sociales", publicación de la Universidad Autónoma Metropolitana plantel Xochimilco.

España. Ministerio de Defensa. "Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio". Madrid. 2011. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf Página en castellano. Fecha de captura: 07/06/12.

España. Ministerio de Defensa. "Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio". Madrid. 2011. Disponible en: http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&sqi=2&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.defensa.gob.es%2Fceseden%2FGalerias%2Fdestacados%2Fpublicaciones%2Fmonografias%2Fficheros%2F128_LOS_AMBITOS_NO_TERRESTRES_EN_LA_GUERRA_FUTURA_ESPACIO.PDF&ei=TfZyUJjUAo7o8QT14IGoBA&usg=AFQjCNFjpOE_QSyYTKRRvxbH0i69xJebKw Página en castellano. Fecha de captura: 07/06/12.

FOJÓN, Enrique y SANZ, Ángel. “Ciberseguridad en España: una propuesta para su gestión”, Análisis del Real Instituto Elcano, ARI Nº 101/2010.

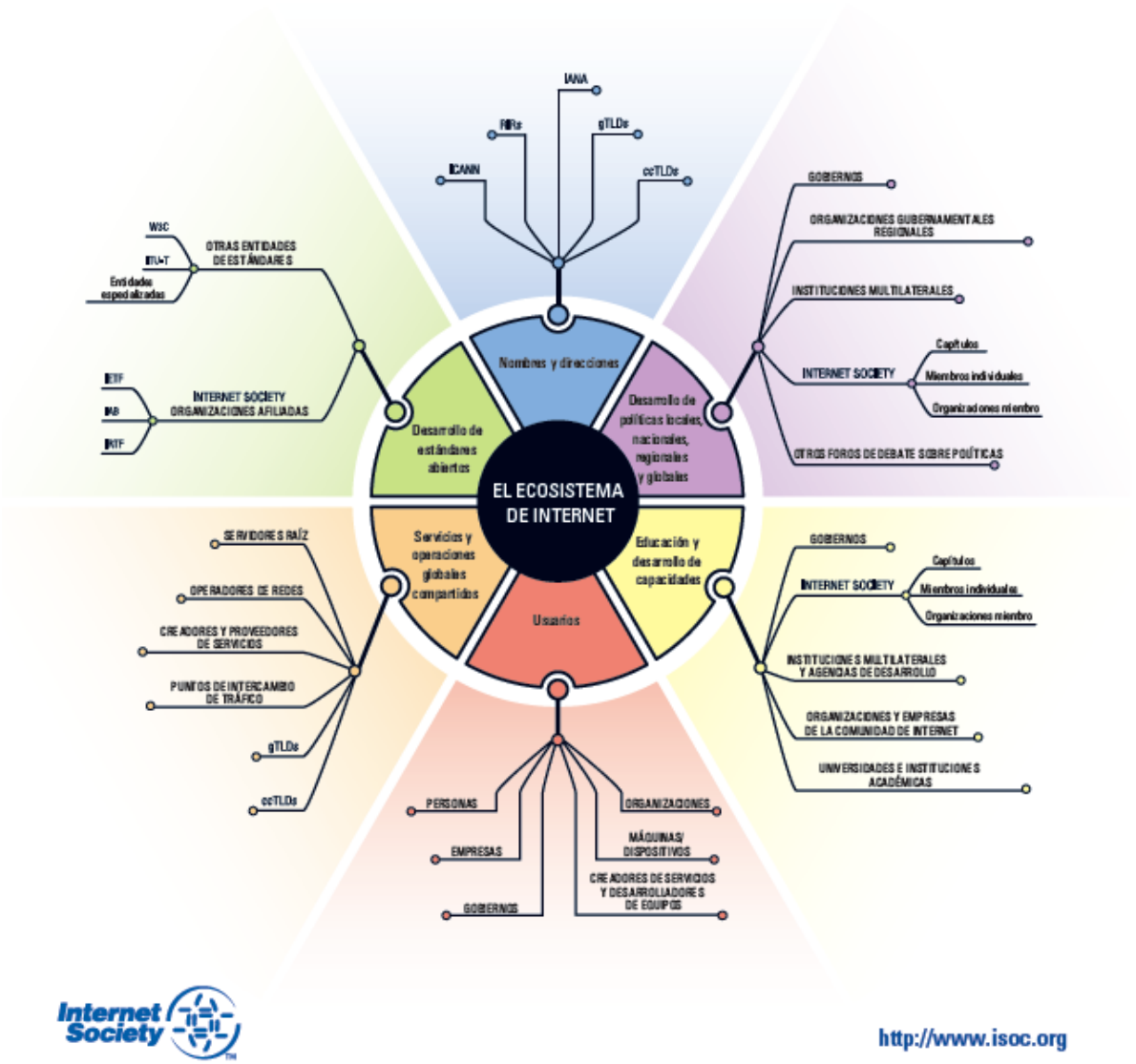
UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Comisión de Estudio 2-3er Periodo de Estudios (2002-2006) “Informe sobre las infraestructuras nacionales de seguridad del Ciberespacio” Ginebra 2006.
http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&sqi=2&ved=0CC0QFjAC&url=http%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-d%2Fopb%2Fstg%2FD-STG-SG02.09.1.3-2006-PDF-S.pdf&ei=e_RyULXeKYLa8ATFhYD4Bg&usg=AFQjCNFjRo6pF733dZ66JlzfIzDZSGg2Dg Página en castellano. Fecha de captura: 07/06/12.

ANEXO A

El ecosistema de Internet

Internet es exitosa en gran parte gracias a su modelo único: la propiedad global compartida, el desarrollo basado en estándares abiertos y los procesos de acceso libre para el desarrollo de tecnologías y políticas.

El éxito sin precedentes de Internet continúa su marcha porque el modelo de Internet es abierto, transparente y colaborativo. El modelo se basa en procesos y productos que son locales, ascendentes (bottom-up) y accesibles para usuarios de todo el mundo.



Internet Society

http://www.isoc.org

Los **County-Code Top-Level Domains (ccTLDs)** ccTLDs se operan según las políticas locales que normalmente se adaptan al país o al territorio en cuestión. *http://www.iana.org/domains/root/db/*

Los registros de **Generic Top-Level Domains (gTLDs)** gTLD operan dominios de nivel superior genéricos patrocinados y no patrocinados según las políticas de ICANN. *http://www.iana.org/domains/root/db/#*

Gobiernos Los gobiernos federal, estatal y local y sus reguladores cumplen funciones para establecer políticas que abarcan desde la implementación de Internet hasta su uso.

Organizaciones gubernamentales regionales Las organizaciones gubernamentales regionales incluyen, entre otras, la Unión Africana, Cooperación Económica de Asia-Pacífico (APEC), la Telecomunidad de Asia-Pacífico, la Unión de Telecomunicación del Caribe (CTU), la Confederación de Naciones, la Unión Europea (EU) y la Comisión Interamericana de Telecomunicación (CITEL). A veces, a los gobiernos les complace coordinar políticas relacionadas con Internet para sus regiones.

Internet Architecture Board (IAB) La IAB está constituida como comité de la Internet Engineering Task Force (IETF) y es una entidad de asesoramiento de la Internet Society (ISOC). Entre sus responsabilidades se incluyen la supervisión de la arquitectura de las actividades de la IETF, la supervisión y la apelación de los procesos de estándares en Internet y el nombramiento del RFC Editor. La IAB también es responsable de gestionar los registros de parámetros de los protocolos de la IETF. *http://www.iab.org/*

Internet Assigned Numbers Authority (IANA) IANA es responsable de la coordinación de la raíz de sistema de nombres de dominios (DNS), las direcciones de protocolo de Internet (IP) y otros recursos relacionados con estos protocolos. *http://www.iana.org/*

Internet Corporation for Assigned Names and Numbers (ICANN) ICANN es una corporación de beneficio público sin fines de lucro que coordina el sistema de nombres y números únicos que son necesarios para mantener Internet segura, estable y interoperable. Promueve la competencia y desarrolla políticas sobre los identificadores únicos de Internet mediante su función de coordinación del sistema de nombres de Internet. *http://www.icann.org/*

Internet Engineering Task Force (IETF) La IETF es una extensa comunidad abierta e internacional de diseñadores de redes, operadores, proveedores e investigadores relacionados con la evolución de la arquitectura y el funcionamiento estable de Internet. Está abierta para cualquier persona interesada. *http://www.ietf.org/*

Organizaciones y empresas de la comunidad de Internet Muchas organizaciones y empresas de Internet fomentan, capacitan e invierten en educación y desarrollo de capacidades para Internet. Entre las organizaciones se incluyen, sin limitarse a ellas, los RIR, los operadores de redes regionales y nacionales y el Network Startup Resource Centre (NSRC), además de proveedores como Afilias Limited, Alcatel-Lucent, Cisco, IBM y Microsoft.

Internet Research Task Force (IRTF) La misión de la IRTF es promover la investigación relevante para el desarrollo futuro de Internet mediante la creación de grupos de investigación concentrados, a largo plazo y pequeños, que trabajen en temas relacionados con los protocolos, las aplicaciones, la arquitectura y la tecnología de Internet. *http://www.irtf.org/*

Internet Society (ISOC) La ISOC promueve la evolución y el crecimiento de la Internet global. Mediante miembros, secciones y socios, es el centro de la red internacional más grande de personas y organizaciones que trabajan con Internet. *http://www.isoc.org*

Capítulos de ISOC Los capítulos de ISOC localizan los valores fundamentales de ISOC y promueven la Internet en las comunidades locales. *http://www.isoc.org/isoc/chapters/*

Miembros individuales de ISOC Los miembros individuales de ISOC demuestran compromiso con la visión de ISOC. *http://www.isoc.org/members/*

Organizaciones miembro de ISOC Las organizaciones miembro de ISOC respaldan a ISOC y contribuyen con ella, y comprenden la necesidad de actuar colectivamente para garantizar que Internet permanezca abierta, accesible, confiable y segura. *http://www.isoc.org/orgs/*

International Telecommunication Union Telecommunication Standarization Sector (ITU-T) La ITU-T convoca regularmente a especialistas de la industria, del sector privado y de entidades de investigación y desarrollo de todo el mundo para desarrollar especificaciones técnicas que garanticen que todas las partes de los sistemas de comunicaciones puedan interoperar sin fisuras con los diversos elementos que conforman las complejas redes y los complejos servicios de ICT de la actualidad. *http://www.itu.int/ITU-T/*

Puntos de intercambio de tráfico (IXP) Los IXP regionales y nacionales proporcionan la infraestructura física que permiten que los operadores de redes intercambien el tráfico de Internet entre sus redes mediante acuerdos de pares mutuos.

Instituciones multilaterales y organismos de desarrollo Las instituciones multilaterales incluyen organizaciones con múltiples países que trabajan en conjunto sobre temas relacionados con Internet para el desarrollo de políticas, la educación y el desarrollo de capacidades. Entre las organizaciones se incluyen, sin limitarse a ellas, la International Telecommunication Union (ITU), el ITU's Development Sector (ITU-D), la United Nations' UNESCO y la World Intellectual Property Organization (WIPO).

Operadores de redes Los operadores de redes incluyen empresas que proporcionan acceso a Internet. Los Regional Network Operator Groups (NOGs) proporcionan colaboración y oportunidades de consulta para operadores locales y globalmente entre los NOG.

Otros foros de debate de políticas Las organizaciones incluyen, sin limitarse a ellas, el Internet Governance Forum (IGF) y la Organisation for Economic Co-operation and Development (OECD), además de foros nacionales de consulta, asociaciones de la industria y organizaciones de la sociedad civil.

Regional Internet Registries (RIRs) Los RIR supervisan la asignación y el registro de los recursos de los números de Internet en una región específica del mundo. Todos los RIR son miembros de la Number Resource Organization (NRO). Los RIRs incluyen AfriNIC, el Asia Pacific Network Information Centre (APNIC), el American Registry for Internet Numbers (ARIN), el Latin American and Caribbean Internet Addresses Registry (LACNIC) y el RIPE Network Coordination Centre. *http://www.nro.net/*

Servidores raíz Los servidores raíz de nombre DNS publican de manera confiable el contenido de un pequeño archivo denominado zona raíz en Internet. Este archivo está en la parte superior de una base de datos con distribución jerárquica denominada sistema de nombres de domino (DNS), que es usada por prácticamente todas las aplicaciones de Internet para traducir nombres únicos de todo el mundo, como www.isoc.org, en otros identificadores. La Web, el correo electrónico y otros servicios usan DNS. *http://www.root-servers.org/*

Creadores/proveedores de servicios Los creadores y proveedores de servicios proporcionan aplicaciones y experiencias de software que usan Internet.

Entidades de estándares especializadas Muchas organizaciones se concentran en estándares especializados y algunas cumplen funciones clave en Internet. Estas organizaciones incluyen, sin limitarse a ellas, el European Telecommunications Standards Institute (ETSI), Identity Commons, la IEEE Standards Association, ISO ANSI, Liberty Alliance Project, comunidades de código abierto y la Organization for the Advancement of Structured Information Standards (OASIS).

Universidades e instituciones académicas Históricamente, tal como en la actualidad, las instituciones académicas cumplen una función crítica en la educación de estudiantes y ejecutivos. También realizan prototipos y demostraciones en soluciones de hardware y software que benefician a Internet.

Usuarios Personas y organizaciones que usan Internet o les proporcionan servicios a otras personas por Internet.

World Wide Web Consortium (W3C) W3C es un consorcio internacional en el que las organizaciones miembro, el personal a tiempo completo y el público trabajan juntos para desarrollar estándares para la Web. *http://www.w3.org*

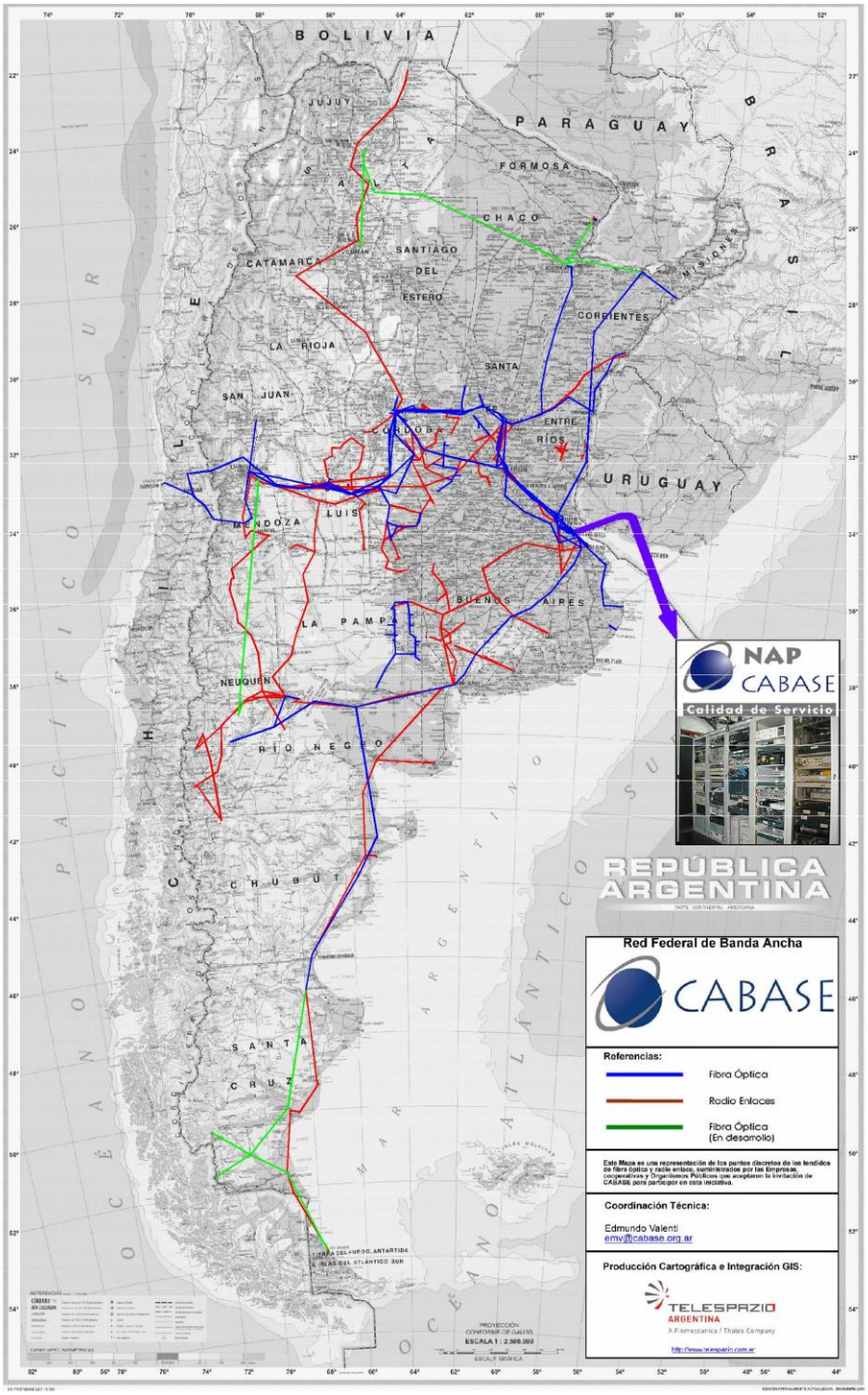
Internet Society es una organización sin fines de lucro fundada en 1992 como líder para promover la evolución y el crecimiento de Internet. Mediante miembros, capítulos y socios, somos el centro de la red internacional más grande de personas y organizaciones que trabajan con Internet. Trabajamos a muchos niveles para ocuparnos del desarrollo, la disponibilidad y la tecnología de Internet.

1775 Wiehle Avenue, Suite 201, Reston, VA 20190-5108, U.S.A.
+1 703 439 2120

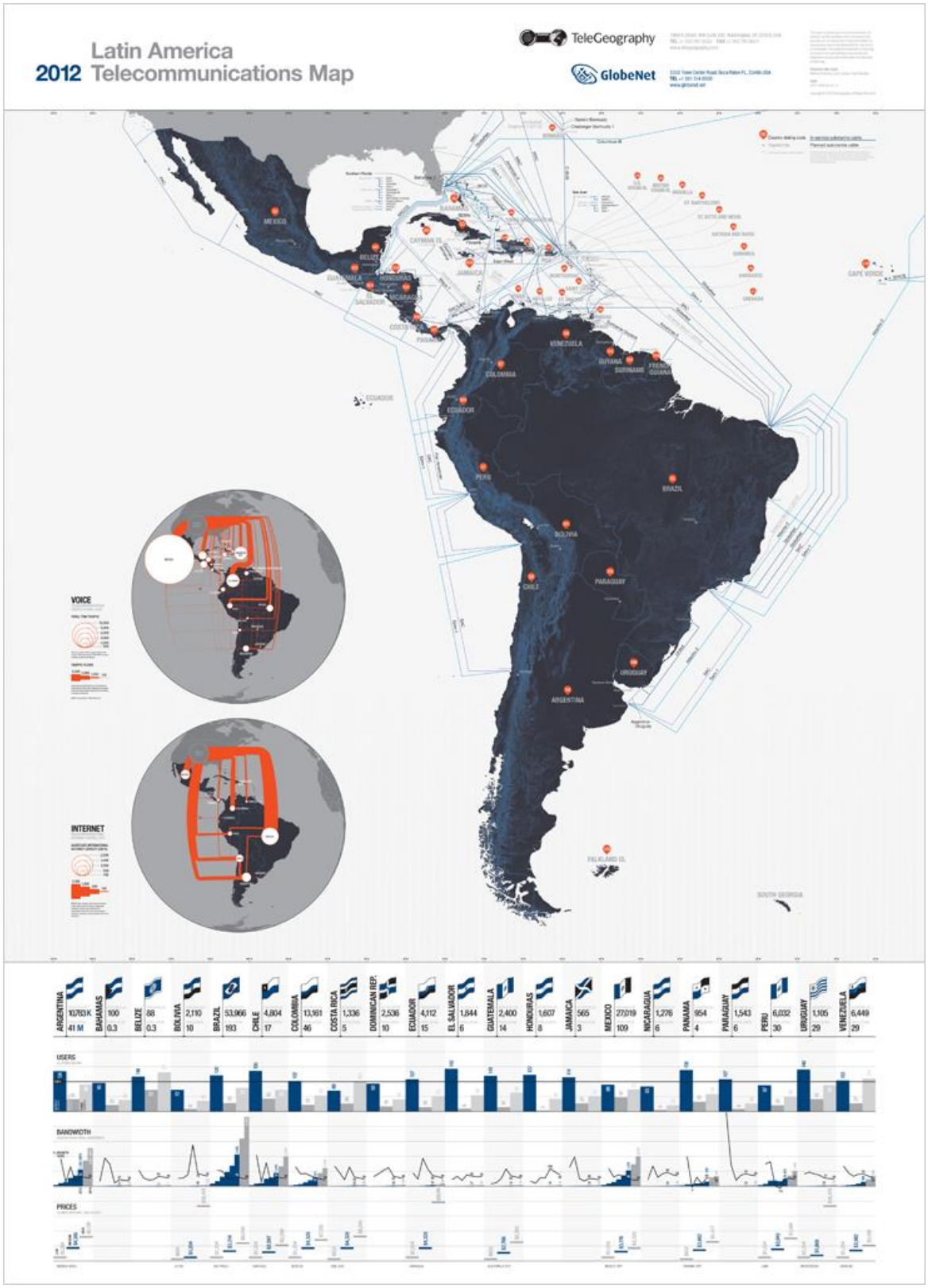
Galerie Jean-Malbuisson 15, CH-1204 Genève, Switzerland
+41 22 807 1444

03/24

ANEXO B


BOLIVIA
PARAGUAY
BRASIL
JUJUY
FORMOSA
CHACO
SANTIAGO DEL ESTERO
CATAMARCA
CORRIENTES
LA RIOJA
SANTA FE
SAN JUAN
CORDOBA
ENTRE RIOS
URUGUAY
MENDOZA
SAN LUIS
BUENOS AIRES
LA PAMPA
NEUQUEN
RIO NEGRO
CHUBUT
SANTA CRUZ
TIERRA DEL FUEGO, ANTARTIDA E ISLAS DEL ATLANTICO SUR
OCEANO PACIFICO SUR
OCEANO ATLANTICO SUR
MAR ARGENTINO
NAP CABASE
Calidad de Servicio
REPUBLICA ARGENTINA
Red Federal de Banda Ancha
CABASE
Referencias:
Fibra Óptica
Radio Enlaces
Fibra Óptica (En desarrollo)
Este Mapa es una representación de los puntos discretos de los tendidos de fibra óptica y radio enlace, suministrados por las Empresas, cooperativas y Organismos Públicos que aceptaron la invitación de CABASE para participar en esta iniciativa.
Coordinación Técnica:
Edmundo Valenti
emv@cabase.org.ar
Producción Cartográfica e Integración GIS:
TELESPAZIO ARGENTINA
A Finmeccanica / Thales Company
http://www.telespazio.com.ar

ANEXO C


Latin America
2012 Telecommunications Map
TeleGeography
GlobeNet
MEXICO
BELIZE
GUATEMALA
HONDURAS
EL SALVADOR
NICARAGUA
COSTA RICA
PANAMA
CAYMAN IS.
JAMAICA
VENEZUELA
GUYANA
SURINAME
FRENCH GUIANA
COLOMBIA
ECUADOR
PERU
BRAZIL
BOLIVIA
PARAGUAY
CHILE
URUGUAY
ARGENTINA
FALKLAND IS.
SOUTH GEORGIA
CAPE VERDE
GRENADA
VOICE
INTERNET
ARGENTINA 10783 K 41 M
BAHAMAS 100 0.3
BELIZE 88 0.3
BOLIVIA 2,110 10
BRAZIL 53,966 193
CHILE 4,804 17
COLOMBIA 13,161 46
COSTA RICA 1,336 5
DOMINICAN REP. 2,536 10
ECUADOR 4,112 15
EL SALVADOR 1,844 6
GUATEMALA 2,400 14
HONDURAS 1,607 8
JAMAICA 565 3
MEXICO 27,019 109
NICARAGUA 1,276 6
PANAMA 954 4
PARAGUAY 1,543 6
PERU 6,032 30
URUGUAY 1,105 29
VENEZUELA 6,449 29
USERS
BANDWIDTH
PRICES

DEFINICIONES

Infraestructuras Críticas: son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información situado en el Sector Público Nacional, Organismos Provinciales, Municipales u Organismos Privados cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad, la información, la integridad física o el bienestar económico y social de los ciudadanos o en el eficaz funcionamiento de las instituciones estatales y las administraciones públicas.[41]

Cibercombatiente: aquel combatiente con saberes específicos, que formando parte de las Fuerzas Armadas participa de una guerra cibernética, y basándose en un plan, emplea las capacidades ciberespaciales del sistema de defensa para atacar objetivos militares del enemigo y proteger los intereses vitales propios.[42]

[41] Jefatura de Gabinete de Ministros. "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC) http://www.icic.gob.ar/paginas.dhtml?pagina=180

[42] Definición efectuada por el autor del presente estudio.

Acrónimos

ADSL	Asymmetric Digital Subscriber Line – Línea de abonado digital asimétrica
ARIU	Red de Interconexión Universitaria
CABASE	Cámara Argentina de Bases de Datos y Servicios en Línea.
CNC	Comisión Nacional de Comunicaciones
CSIRT	Computer Security Incident Response Team - Centros de Respuesta a Incidentes de Seguridad Informática
DIH	Derecho Internacional Humanitario
DNS	Domain Name System – Servidor de Nombres de Dominio
GTIC	Grupo de Tecnologías de la Información y las Comunicaciones
ICANN	Internet Corporation for Assigned Names and Numbers – Corporación para la asignación de nombres y números Internet
IAB	Internet Architecture Board – Junta de Arquitectura de Internet
IETF	Internet Engineering Task Force – Grupo Especial sobre Ingeniería de Internet
IP	Internet Protocol – Protocolo Internet
ISP	Internet Service Provider – Proveedor de Servicios de Internet
ISOC	Internet Society – Sociedad de Internet
LACNIC	Latin America and some Caribbean Islands – Latinoamérica y algunas Islas del Caribe
NAP	Network Access Point – Punto de Acceso a Internet
NIC	Network Information Center – Centro de Información de Redes
ONTI	Oficina Nacional de Tecnologías de Información
ONU	Organización de las Naciones Unidas
POP	Point of Presence – Punto de Presencia
RIR	Regional Internet Register – Registro Regional de Internet
TELCOs	Telecommunications Companies – Companias de Telecomunicaciones
TIC	Tecnologías de la Información y la Comunicación
UIT	Unión Internacional de Telecomunicaciones
W3C	World Wide Web Consortium – Consorcio World Wide Web