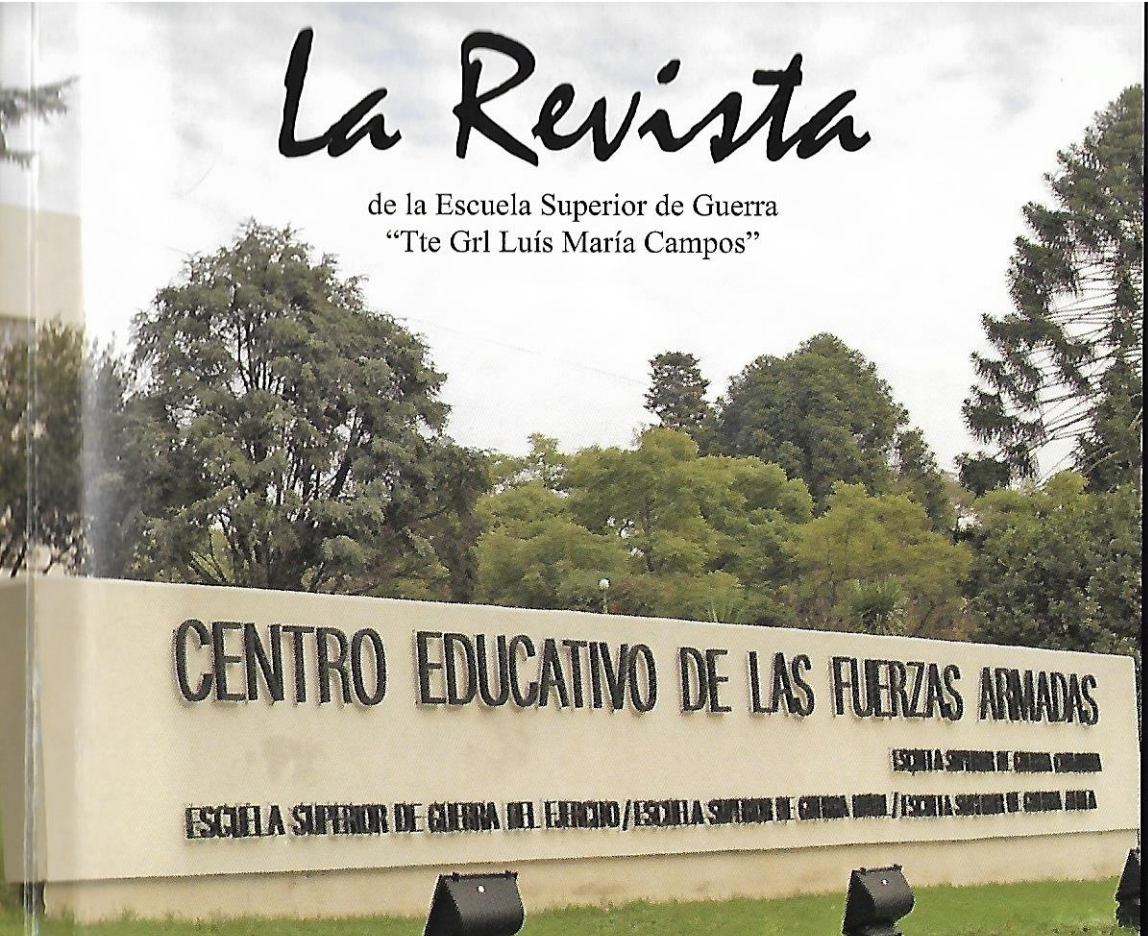
La Revista

de la Escuela Superior de Guerra
"Tte Grl Luís María Campos"



EJÉRCITO ARGENTINO

Director ESG y Director de la Revista
Cnl Federico Sidders

Secretario de la Revista
Cnl (R) Justino M. Bertotto

Diseño Gráfico
A/C María Camila Serrano

Encargado de la Revista y Corrección
Prof. Carlos Raúl G. Gutiérrez

Auxiliar de Archivo
Sol Vol Téc Lucio Trimarco

Suscripción Anual en
Luís María Campos 480
1426 - Ciudad Autónoma de Buenos Aires
(011) 4-576-5689 Int 6004
Descuento por MUPIM

Propiedad Intelectual
Nro. 191840
ISSN 0327-1137

Impreso en
Arsa Gráfica

SEP - DIC 12 Nro 582

SUMARIO

Estrategias de Defensa Cibernética en la Era de la Información

Doctor J. Ulises Ortiz

Introducción

En 1982, la Guerra del Atlántico Sur fue el bautismo de fuego del Arma de Comunicaciones del Ejército Argentino[1], junto con componentes de esa especialidad de la Fuerza Aérea y la Armada Argentina. Este accionar en las Islas Malvinas como desde el Continente y a través de medios aéreos así como desde buques de superficie y en submarinos, evidenció los primeros indicios de la nueva Revolución de la Informática en los Asuntos Militares en Argentina. Aplicada al avance de las telecomunicaciones como inicio de los sistemas de información, esta revolución tecnológica hoy requiere de nuevas y complejas configuraciones organizacionales[2].

Al presente, es un hecho insoslayable que nos encontramos no sólo en un nuevo siglo sino que la era industrial (que va desde la invención de la máquina a vapor y su segunda fase con el desarrollo del motor a combustión) ha dejado lugar a la denominada era de la información, sustentada sobre los avances tecnológicos. Ésta, entendida como el impacto de las telecomunicaciones y la informática conforma la infraestructura tecnológica de la globalización que hace posible la toma de decisiones estratégicas en tiempo real a una escala global. En este sistema de producción integrado-transnacional participan juntos a los Estados, decenas de miles de empresas altamente tecnológicas de carácter mundial con centenares de miles asociadas. En respuesta a ello, surgen innovadores conceptos como "Estado Digital"[3] o en el denominado "Estado-Red"[4], adaptado a los requerimientos de esta nueva era donde la soberanía pasa a ser no solo territorial sino "espacial". Estos cambios económicos, tecnológicos, políticos y organizacionales impactaron también en lo social, creando inclusión o exclusión respecto de sus beneficios así como en las estructuras de defensa de los Estados.

---

1 Estado Mayor General del Ejército. Historia de las comunicaciones en el Ejército Argentino, Tomo II, Comisión Arcángel San Gabriel. 2000.

2 Como el denominado, entre otros, C4ISTAR (centro de comando y control, comunicaciones, computadoras, inteligencia, vigilancia, adquisición de objetivos y reconocimiento) en su relación con las infraestructuras militares que lo soportan.

3 G. Keyworth y otros, The Digital State: How State Governments are Using Digital Technology, Executive Summary (Washington, DC: The Progress and Freedom Foundation, September 1998). URL: http://www.pff.org/digital98.html.

4 Castells, Manuel: "¿Hacia el Estado Red?: Globalización económica e instituciones políticas en la era de la información", Seminario Internacional Sociedade e a Reforma do Estado, ponencia en Brasil, San Pablo, marzo de 1998.

La Protección de las Infraestructuras Críticas

Las nuevas tecnologías se asientan en el espacio urbano. Allí se estructuran los nodos de las infraestructuras críticas dadas por el complejo tecnológico-electrónico-informacional así como la compleja logística que supone sostener los requerimientos de subsistencia de las grandes concentraciones urbanas y la administración de sus recursos. Por lo tanto, la concentración urbana crea un nuevo espacio "las megalópolis" constituyéndose en ellas sistemas "metaestables" que las sostienen y por ello verdaderamente críticos.

La Oficina de Protección de la Infraestructura Crítica de los Estados Unidos (EUA) entiende por "infraestructura crítica" (IC) a los sistemas que tienen incapacidades o podrían ser debilitados o destruidos con impacto en la defensa y seguridad económica de la nación, incluyendo bancos, transporte, sistemas de agua, servicios del gobierno y gobiernos públicos[5].

En virtud de estos nuevos espacios, resurgen correlativamente en la agenda de defensa los objetivos de preservar recursos estratégicos como el agua (el control y aseguramiento de sus fuentes), los alimentos, las fuentes de energía, etc. claramente identificados por el asesor en temas de defensa en Francia Philippe Delmas en su clásico "El brillante porvenir de la Guerra"[6]. Para Delmas, ese "porvenir", estará dado por nuevos conflictos por la necesidad de agua, alimentos, su transporte, etc. En términos del presente enfoque, esos objetivos se encuentran directamente asociados a los nodos ya que los sistemas de aprovisionamiento de agua, las redes de producción y distribución de energía, etc., están integradas al sistema informacional para su control y distribución. Así, ese nuevo "campo", demanda sistemas de protección, previsión, aseguramiento y defensa contra los riegos y catástrofes provocados por incidentes no intencionales, intencionales o desastres. Para Manuel Castells el atentado 0911 en Nueva York fue el inicio de la primera guerra mundial del siglo XXI, la "guerra red", que busca "imponer sus objetivos utilizando las únicas armas eficaces en su situación de inferioridad tecnológica y militar"[7].

Las Ciberguerras

La era de la información posee un nuevo "espacio" informacional y una infraestructura "crítica" que lo soporta, demandando esfuerzos en igual sentido. Los nuevos conflictos de esta era han dado lugar a la denominada guerra de la información, donde se ataca el nudo o "nodo" que hace al control, la comunicación, administración, comercialización, etc., esto es, las redes informáticas y las infraestructuras que las soportan. No se trata solamente de poder atacar un pozo petrolero

5 Plan of "Critical Infrastructure Assurance Office" (CIAO); Strategy to Secure Cyberspace -NSSC) y **National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.**
6 Delmas, Philippe. El Brillante porvenir de la Guerra. Chile. Editorial Andrés Bello. 1995.
7 Castells, Manuel. La Guerra Red. Diario "El País". Madrid. 6/02/02.

para evitar el flujo de combustible como era un ataque en la transición de la era industrial a la nueva era. Se trata de atacar un centro financiero, un sistema de comunicaciones gubernamental o infectar una red de computadoras vinculadas a la defensa, afectando así al sistema de una nación, desarticulando sus capacidades.

Por tal motivo, las estrategias nacionales, bilaterales y multilaterales en esta materia se orientan hacia la identificación y protección de las infraestructuras críticas de cada nación y región en la faz pública y por medio de acciones conjuntas con empresas en lo privado.

Nicolás Arpagian, especialista en ciberseguridad, redactor de la revista francesa Prospectiva Estratégica y autor de "La Cyberguerre, la guerre numérique a commencé"[8] indica que fue Norbert Winer (1894-1964), profesor del Massachussets Institute of Technology (MIT) quien en 1964 creó el término "cibernética" al designar la disciplina que estudia el problema del control y la comunicación en general y William Gibson, autor de obras de ciencia ficción, quien desarrollará en 1984 el término "ciberespacio" como un lugar indefinido en el mundo que existe y donde millones de personas viven a diario.

Por su parte, Francois-Bernard Huyghe, especialista francés en ciencias de la información estratégica desarrollará la distinción entre:

- Ciberguerra (cyberwar – information warfare): que se orienta estrictamente a la conducción de operaciones militares según los principios relativos de los canales de información, tendientes a destruir o controlar los sistemas de comunicación del adversario y,
- Netguerra (netwar): corresponde a los conflictos a gran escala entre naciones o sociedades comerciales. En este caso el agresor va a buscar modificar o pervertir lo que una población civil (consumidores, opinión pública, electores, clientes, etc.) saben o creen de ella misma o del mundo que lo rodea[9].

Esta distinción es coincidente con la perspectiva estadounidense de John Arquila y David Ronfeldt, investigadores estadounidenses, quienes en su clásico en la materia "Networks y Netwars"[10] preparado para la Secretaría de Defensa de EUA en 2001, analizan la agenda de los conflictos por desarrollarse en el ciberespacio producto de la globalización y como enfrentarlos. En tal sentido asignaban una especial importancia a la defensa de las "infraestructuras tecnológicas" que las soportan.

Para el académico Joseph Nye, ex asistente al Secretario de Defensa de EUA, "la ciberguerra es una acción hostil en el ciberespacio cuyos efectos amplían o son equivalentes a una violencia física importante. En el mundo físico, los gobiernos ejercen prácticamente un monopolio en el uso de fuerza a gran escala, el defensor

8 Ed Magnard-Vouibert. París. 2009.
9 Idem, 7 pág 24.
10 RAND Co. - National Defense Research Institute. California. 2001

tiene un conocimiento íntimo del terreno y los ataques terminan como consecuencia del desgaste o del agotamiento. Tanto los recursos como la movilidad son costosos"[11]. Nye entiende que países como EUA, Rusia, Gran Bretaña, Francia y China tienen una capacidad mayor que otros estados y actores no estatales para controlar el mar, el aire o el espacio, pero casi no tiene sentido hablar de predominio en el ciberespacio, porque la dependencia de sistemas cibernéticos complejos para el respaldo de actividades militares y económicas crea nuevas vulnerabilidades en los estados grandes.

Por ello, el referido Arpagian expone que "la ciberguerra irrumpió en nuestras sociedades para incrustarse en todos los campos, desde el militar hasta el civil. Las redes informáticas provocaron una suerte de extensión de los campos de batalla hacia un mundo virtual en plena interacción con la realidad"... "la ciberguerra pone en tela de juicio los fundamentos mismos de la forma de hacer la guerra. La ciberguerra obtiene resultados importantes a bajo costo. Es más barato movilizar 10.000 computadores que 10.000 soldados. La tecnología de las redes reequilibra la geopolítica12". Así, Arpagian indica que insurgentes iraquíes el 18 de diciembre de 2009 lograron hachear sistemas de operaciones militares de los aviones Predator de los EUA por medio de un software informático que no cuesta más de 26 U$S. El gran objetivo de este nuevo tipo de guerra (guerra "no guerra" al decir de Alvin Toffler13) es la destrucción de las capacidades informacionales y las infraestructuras críticas. Esta concepción de la guerra como "no solo militar" ha sido desarrollada en otras partes del planeta. Diversos documentos en EUA, Europa y otros países como India, Rusia y China, comienzan a conceptualizar estratégicamente sobre el tema y generar acciones. De este modo el espacio informacional y la infraestructura "física" crítica se encuentran en una concepción amplia que las interrelaciona estratégicamente.

Actualmente se generan cambios continuos en las estrategias militares, capacidades militares, cambios en las organizaciones, en las operaciones terrestres, y en los procedimientos militares. Estas guerras de "cero bajas" tienen distintos enfoques, pero todas incluyen un punto: el impacto de las tecnologías de la información en el campo militar[14].

En ese sentido, para el experto en redes Jorge Soriano[15], el primer escuadrón en entrar en acción durante una ciberguerra será el de "reconocimiento", teniendo como misiones:

11 http://www.project-syndicate.org/commentary/cyber-war-and-peace/spanish
12 http://www.pagina12.com.ar/diario/elmundo/4-145379-2010-05-09.html
13 Toffler, Alvin y Hedi. Las Guerras del Futuro, la supervivencia en el alba del siglo XXI. Barcelona. Plaza & Janes. 1994.
14 "La OI en el combate asimétrico: opción esencial para una respuesta limitada. Revista del Ejército de España. 2004. Nro 764.
15http://www.realnet.com.mx/index.php/capacitacion/noticias/tendencias/el-mundo-ti-en-numeros/articulos/241-el-arte-de-la-guerra-y-sus-cibercomandos.html

- obtener la mayor cantidad de información posible del adversario con especial interés en el Web e información referente a inversiones en nuevas tecnologías, sistemas, y servicios proporcionados a terceros.
- obtener información de la tecnología utilizada por el enemigo y sus puntos débiles, en este caso direcciones IP, puertos abiertos, servicios, hosts, servidores Web, sistemas operativos, bases de datos, nombres de dominio, servidores de correo electrónico, y en general la tecnología en la cual el enemigo basa sus sistemas de comunicación y operaciones.

Luego el "escuadrón de asalto", compuesto por soldados altamente entrenados, romperá las defensas del enemigo para identificar usuarios válidos en sus sistemas, obtener acceso, escalar privilegios en el sistema, creando "nuevos huecos para poder desplazarse, ocultar cualquier evidencia de su presencia" y, obtener, alterar o destruir la información u operación del sistema. Esta será una guerra con bajas principalmente materiales.

Algunos hechos recientes lo confirman:

2007. En mayo el sistema informático de Estonia es atacado por Internet en un equivalente a la utilización de un millón de computadoras[16]. Estonia queda paralizada durante varias semanas y requerirá la ayuda de la OTAN para recomponer sus sistemas. James Appathurai, vocero de la NATO expresó sobre el ataque que esta situación "no es de tanques y artillería[17]" y tras la reunión de los Jefes de la OTAN a mediados de junio de ese año sintetizó en que "todos estuvieron de acuerdo en que es imprescindible mejorar la capacidad de protección de los sistemas informáticos de importancia crítica[18]".

2008. Coincidiendo con la operación militar rusa en Georgia, varias webs gubernamentales de este país son atacadas con el troyano BlackEnergy, paralizando sistemas informáticos y tomando el control de la web del presidente georgiano.

2009. Soldados estadounidenses desplegados en Irak capturaron a combatientes de un grupo chiíta rebelde con computadoras portátiles con imágenes tomadas por los aviones robot 'Predator'. Según expertos, habían tomado el control del sistema informático de transmisión de las imágenes del avión.

2010. En junio un programa así denominado creado específicamente para tomar control de sistemas que manejan las operaciones internas de plantas industriales ataca a varios países, afectando miles de sistemas informáticos de automatización industrial utilizados en plataformas petroleras, oleoductos, centrales eléctricas y nucleares. Se ven afectados Pakistán, India, China (afectando a 6 millones de

16 http://news.bbc.co.uk/1/hi/world/europe/6665145.stm
17 Idem 7.
18 http://www.lanacion.com.ar/archivo/Nota.asp?nota_id=928136

PC), Indonesia (18% de los ataques), EUA (2%) y en Irán (66%). Se estimó que el control de daños llevó hasta dos meses. En tal sentido, a fines de septiembre de ese año Mahmud Liayi, responsable de tecnología informática del Ministerio de Industria iraní expresó que "una guerra electrónica fue lanzada contra Irán", afectando a 30.000 computadoras en el país, entre ellas el equipo de la central nuclear de Bushehr, inaugurada el un mes atrás.

2011. De acuerdo al Norton Cybercrime Report 2011, el gasto anual mundial en ciberseguridad alcanzó los US$ 114 mil millones. A fines de octubre, se conoce la aparición de un nuevo malware detectado en Irán, Sudán, Francia, Vietnam, India, Suiza, Holanda y Ucrania., llamado Duqu, creado para realizar espionaje industrial y no para arruinar físicamente sistemas industriales y entendido como precursor de un futuro Stuxnet, dado que la información que recolecta sería usada para un nuevo ataque más poderoso.

Estrategias de Defensa Cibernética

En enero de 2012, **el** "Cyber Statecraft Initiative at the Atlantic Council" con sede en Bruselas y la empresa de seguridad cibernética de McAfee realizaron un ranking de países en materia de ciberdefensa.

Resultaron agrupados en 6 grupos (en cada uno por orden alfabético):

1. Finlandia, Israel y Suecia
2. Alemania, Dinamarca, España, Estonia, EUA, Francia, Holanda y Reino Unido
3. Australia, Austria, Canadá y Japón
4. China, Italia, Polonia y Rusia
5. Brasil, India y Rumania
6. México[19].

A modo de ejemplo, cabe destacar el desarrollo de acciones por parte de la OTAN y algunos países.

Un escudo cibernético para la OTAN

En Septiembre de 2010 William J. Lynn, entonces Subecretario de Defensa de los Estados Unidos indicaba en oportunidad de una reunión de la OTAN que esta organización debía construir un "escudo de cibernético" para proteger la alianza transatlántica de cualquier amenaza a sus infraestructuras militares y económicas

19 http://www.acus.org/content/no-nato-members-ranked-among-top-three-cyber-defense

ya que la Alianza tiene un papel crucial que desempeñar en la ampliación de una malla de seguridad sobre nuestras redes". Lynn expresó que "la OTAN tiene un escudo nuclear, está construyendo un escudo de defensa más fuerte y más fuerte, que necesita un ciber-escudo".

EUA crea el Primer cibercomando militar

El 21 de mayo de 2010 se anuncia la creación del Primer cibercomando en EUA (U.S. Cyber Command - USCYBERCOM) bajo el mando del Comando Estratégico militar. Su misión es planear, coordinar, integrar, sincronizar y conducir "actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento 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 EEUU y sus aliados en el ciberespacio y impedir lo mismo a nuestros adversarios". En tal sentido, el Secretario de Defensa de ese país, Leo Panetta indicó, a mediados de Julio de 2011 que un "nuevo Pearl Harbor es un posibilidad real en el mundo actual, como resultado debemos contrarrestar esto agresivamente". Por su parte, el General Keith B. Alexander, Comandante del USCYBERCOM, indicó en julio de 2012 que le "preocupa el paso de los ataques perjudiciales a los destructivos. Creo que están por venir", añadiendo que hay que prepararse para estos ataques[20].

Por su parte, el Ejército de los EUA, crea en octubre de 2010 el U.S. Army Cyber Command (ARCYBER) como componente dependiente del USCYBERCOM. Ubicado en el área de Washington DC, se compone de 21.000 efectivos, militares y civiles destinados en todo el mundo y tiene por misión[21] planificar, coordinar, integrar, sincronizar, dirigir y conducir operaciones y defensa de la red de todas las redes del Ejército y conducirá operaciones en el ciberespacio en apoyo del completo espectro de las operaciones militares para asegurar la libertad de acción de los EUA y sus aliados en el ciberespacio y para rechazar el mismo a los adversarios[22].

El ciber Ejército Azul de la República Popular China

Diversos investigadores de la Academia de Ciencias Miliateres de China, de la Universidad Nacional de la Defensa China y de la Academia de Comando de Comunicaciones de Wuhan han desarrollado en los últimos años estudios sobre la ciberguerra.

20http://www.washingtonpost.com/blogs/2chambers/post/cybersecurity-chief-urges-action-by-congress/2012/07/09/gJQAP4gMZW_blog.html
21 www.arcyber.army.mil
22 http://www.army.mil/article/46012/army-establishes-army-cyber-command/ -

Así, dos expertos militares en electrónica de la referida Academia, los Coroneles Ye Zheng y Zhao Boaxian, han indicado que el uso de Internet en las revueltas desarrolladas en 2011 en el mundo árabe, están asociadas a acciones gubernamentales desde el exterior de esos países, por lo cual China debe erigir una "frontera de Internet" y "defender su soberanía de internet", indicando que "igual que la guerra nuclear fue la guerra estratégica de la era industrial, la ciberguerra se ha convertido en la guerra estratégica de la era de la información y se ha convertido en una forma de batalla que es muy destructiva y concierne a la vida y la muerte de las naciones". Así, en mayo de 2011 el Coronel Geng Yansheng, Vocero del Ministerio de Defensa Chino indicó que "China es relativamente débil en materia de ciberseguridad y ha sido a menudo víctima de ataques en internet", "actualmente, la seguridad en la red se ha convertido en un problema internacional, que no sólo afecta al ámbito social, sino también al sector militar"[23], indicando que su país ha establecido la creación de una unidad de ciberdefensa, denominada el Ejército Azul.

Los expertos de este país incluyen nuevos conceptos dentro de las denominadas "ciberactividades como "cibermobilización", "cibermanipulación", "ciberecluta-miento" que no conforman lo que entendemos por la guerra (ataque y defensa).

Las actividades militares de la Federación de Rusia en el ciberespacio

A principios de 2012, el Ministerio de Defensa ruso publicó en su página web un documento titulado *"***Criterios conceptuales sobre la actividad de las Fuerzas Armadas de la Federación de Rusia en el espacio informático"**, el cual establece las tendencias que adoptarán sus fuerzas para el control, la prevención y la solución de los conflictos cibernéticos que puedan surgir[24]. Asimismo, el documento indica la posibilidad que ocurran ataques ofensivos contra otros países y propone que se extienda la costumbre del Derecho Internacional en materia de guerras interestatales -como el uso proporcional de la fuerza y la minimización de daños a civiles- a los conflictos en el ciberespacio.

En tal sentido, Eugene Kaspersky director de la compañía rusa de seguridad informática que lleva su nombre hizo una evaluación en relación a los nuevos tipos de ataques de virus como Stuxet o Flame contra infraestructuras críticas como las centrales nucleares o refinerías petroleras. En una conferencia sobre seguridad y ciberespacio desarrollada a mediados de 2012 por la Universidad de Tel Aviv indicó "créame, tengo mucho miedo y preocupación por lo que puede provocar la

23 http://www.offnews.info/verArticulo.php?contenidoID=31344
24 http://rusiahoy.com/articles/2012/07/03/los_peligros_de_la_ciberguerra_17711.html

ciberguerra, espero que se actúe antes de que sea demasiado tarde"[25]. Kaspersky evaluó que para crear un virus como Flame "se necesitó menos de 100 millones de dólares" para pagar a ingenieros, expertos, analistas, técnicos, maquinas de café, etc. y que ese virus "es un ejemplo que el caber-arma es muy peligroso y puede hacer mucho daño, ya no lo llamo ciberguerra sino ciberterrorismo. No sabes dónde y cuándo será el próximo ataque y, si no se actúa rápido, las cosas irán peor. Los países no tienen suficientes defensas" y concluyó que teme "el fin del mundo que conocemos si no hay cooperación internacional contra este peligro".

Las Fuerzas de Defensa de Israel (FDI) y la ciberdefensa

En la mencionada Conferencia de Tel Aviv, el Ministro de Defensa isarelí, Ehud Barak, indicó que su país desarrolla acciones tanto la defensa como el ataque en el ciberespacio, expresando que "a diferencia de la guerra convencional, en este tipo de lucha es más importante invertir en la defensa que atacar al enemigo"[26]. Asimismo, indicó que *"***debemos cambiar a un sistema proactivo, en que no solo reaccionemos ante ataques***"*, agregando que la ciberdefensa *"***es más importante y más difícil***"* que los ciberataques, señalado que Israel desde aspirar a convertirse en líder mundial en ciberdefensa, a niveles militar y civil[27].

El Gobierno israelí estableció a mediados de 2012 un Comité Nacional para desarrollar la defensa de la infraestructura crítica, sistemas financieros y otros activos. Por su parte, las FDI cuentan con componentes específicos frente a ataques tecnológicos contra su país. En abril de 2012, alrededor de 30 efectivos de las FDI se graduaron del su primer curso de los ciber-defensores, desarrollado para brindar capacidades para prevenir los ciberataques contra las redes propias. En el curso estrenaron un nuevo sistema de simulación de ciberguerra denominado Elbit. El simulador, desarrollado para el gobierno, instalaciones militares e instalaciones civiles de infraestructura crítica, permite la formación personal y grupal de los diferentes usuarios en la localización, manejo y gestión de diversos eventos de la guerra cibernética y los ataques que esta trae aparejados. Asimismo ofrece capacitación en prevención de los episodios de guerra cibernética, mediante la simulación de escenarios de redes de protección[28].

25 http://www.elmundo.es/elmundo/2012/06/07/navegante/1339045745.html
26 Idem 23.
27 http://www.ft.com/cms/s/0/43f199f2-afec-11e1-b737-00144feabdc0.html#axzz24l1VdymF
28 http://noti.hebreos.net/enlinea/2012/06/19/9050

El Consejo Superior del Ciberespacio y el Ejército cibernético de Irán

En octubre de 2011, el general Gholam Reza Jalali, Director de la Organización de Defensa Pasiva de Irán, anunció en la conferencia de Defensa Cibernética celebrada en Teherán que para contrarrestar posibles amenazas externas sobre sus instalaciones nucleares, Irán había puesto en marcha un "cibercomando" dedicado a luchar contra posibles ataques de piratas informáticos contra las redes del país, que tendría como misión "vigilar, identificar y contraatacar cuando se produzcan amenazas informáticas contra las infraestructuras nacionales". Jalali indicó que "los Estados Unidos está reduciendo el tamaño de su Ejército para poder tener un infraestructura de defensa cibernética más grande. Pues, países como Irán tienen que instalar y modernizar sus sedes de defensa cibernética e incluso (constituir) un Ejército cibernético". El general iraní expresó también que Irán es uno de los países que más ha sido objeto de ciberataques a lo largo de los últimos dos años. En este sentido, recalcó que los centros atacados no salieron afectados y de momento Irán es en gran medida inmune de este tipo de ataques[29]. A principio de marzo de 2012, el líder iraní ayatolá Ali Jamenei, anunció la creación del **Consejo Superior del Ciberespacio**, conformado por el Presidente del país y los jefes del Parlamento y el Poder Judicial, el secretario del Consejo Supremo de Seguridad Nacional, varios ministros y mandos militares y policiales.

Reino Unido de Gran Bretaña (RUGB)

En un informe de julio de 2010 presentado al Parlamento Británico por el director del Centro de Comunicaciones Gubernamental (GCHQ), de que las amenazas cibernéticas son "reales y creíbles" e indicaba que el RUGB debe prepararse para participar en una serie de operaciones ofensivas cibernéticas para proteger sus intereses. Correspondiente a ello, la Estrategia de Seguridad Británica, publicada en octubre de ese año identificará a la amenaza cibernética, entendida como un ataque hostil sobre el ciberespacio nacional por otros Estados o por el crimen organizado como uno de los cuatro riesgos de nivel I (de mayor probabilidad e impacto), junto a acciones del terrorismo internacional, un accidente importante o un desastre natural que precisa una respuesta nacional, una pandemia o una crisis militar internacional entre estados, afectando al país y sus aliados, así como a actores estatales y no estatales[30].

En tal sentido, el RUGB cuenta con el Programa Nacional de Seguridad Cibernética, tendiente a ampliar los sistemas de protección de la seguridad cibernética, en el aseguramiento de la información (Information Assurance); en mejorar la detección y análisis de los ataques cibernéticos; en aumentar la cooperación con países aliados; y en la creación de una unidad cibernética conjunta en colaboración con el Ministerio de Defensa para desarrollar nuevas tácticas, técnicas y planes relativos a las operaciones militares.

29 http://www.hispantv.com/detail.aspx?id=174671

30http://www.ieee.es/Galerias/fichero/docs_analisis/2010/DIEEEA18-2010EstrategiaNacionalSeguridadBritanica.pdf

La ciberdefensa en Francia

El Libro Blanco sobre Defensa de Francia, aprobado por el Presidente de la República en junio de 2008, puso de relieve como nueva amenaza, el ciberespacio, centrándose en la seguridad de los "sistemas de información, centros nerviosos reales de nuestra sociedad", donde "todos los sectores de actividades, ya sean estatales, industrial, financiero o comercial, dependen más de la tecnología y redes de comunicaciones electrónicas" se verían muy afectados por distinto tipo de disfunciones.

Esa apreciación distingue tres **escenarios** principales:

- un ataque contra los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos: para los militares, es plausible pensar que puedan provocar "en los próximos quince años", provocando destrozos similares o superiores a un bombardeo físico.
- un ataque contra la parte visible de Internet, esto es, las webs y las intranets de administraciones clave, como presidencia, policía, impuestos y hospitales. El hundimiento de esas páginas provocaría caos y desprestigio de un Estado ante sus ciudadanos y ante las potencias extranjeras.
- la integración de cualquiera de esos ataques informáticos en el marco de una secuencia clásica de guerra convencional.

Frente a esta amenaza creciente y aún más insidiosa, el Libro Blanco destacó la necesidad de dotar a Francia "con una capacidad de defensa equipo activa, capaz de detectar y contrarrestar los ataques, recomendando crear agencia nacional responsable. Así, a mediados de 2009 se crea, dependiente del el Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) la Agencia Nacional para la Seguridad de Sistemas de Información (ANSSI) con la misión de proteger los sistemas nacionales de información y proponer las normas que deben aplicarse para la protección de los sistemas estatales y verificar la aplicación de las medidas adoptadas. Por medio del Centro Operacional de la Seguridad de Sistemas de Información (COSSI), se detectan y responden ataques y se vigilan las redes más sensibles de la administración y se desarrollan nuevas capacidades defensivas.

Por su parte el SGDSN mantiene dos planes de trabajo[31]: el Plan Vigipirate de vigilancia, prevención y protección, cuyo principal objetivo es la preparación del Estado para la protección de la población, su infraestructura y sus instituciones, y el Plan de Piranet, complementario del anterior, en respuesta a amenazas o ataques a gran escala utilizando medios específicos de agresión o que afectan a los entornos particulares, donde se requiere la intervención del estado en una grave crisis, constituyéndose así en uno de los pilares de la estrategia de esa defensa. Cabe destacar que en 2012 se anunció que en la escuela interarmas del Ejército francés Saint-Cyr Coëtquida se estableció un centro de conocimientos de ciberdefensa[32].

Alemania

En junio de 2012, un informe al Parlamento del Ministerio de defensa Alemán indicó que desde 2006, el sistema de defensa de ese país posee una unidad militar de operaciones de red de computadoras (Computer Network Operations Unit - CNO) que está subordinada al comando estratégico de inteligencia militar, con sede en Bonn y centrada en la guerra cibernética, logrando capacidad inicial para operar en redes hostiles y desarrollando simulaciones de ataques en un ambiente de laboratorio cerrado. El informe recalca que el desarrollo de la capacidad alemana de ciber-defenderse y ciber-atacar debe ser considerado a la luz de ataques realizados contra redes gubernamentales durante los últimos años y que el país debe ponerse al nivel de otros países de la OTAN, como EUA, Francia y Gran Bretaña[33].

El Hemisferio Americano frente a la ciberseguridad

Los países del Hemisferio en el seno de la Organización de los Estados Americanos (OEA) han definido en los últimos diez años una concepción común en la materia, estableciendo consensos para:

- Un "Enfoque Multidimensional de la Seguridad Hemisférica", procurando proteger la infraestructura crítica y asegurando las redes de los sistemas (2002)[34]
- Contar con "diferentes medios de alerta anticipada que permitirían actuar tratando de evitar atentados a la seguridad y la consiguiente generación de inestabilidad", y fortalecer la coordinación interinstitucional e intergubernamental y de los regímenes de seguridad y defensa en la región que permitan la protección de la población y la estabilidad y la paz", V Conferencia de

31 http://www.sgdsn.gouv.fr/site_rubrique98.html
32 http://defensesystems.com/articles/2012/07/05/agg-france-cyber-warfare-officer-training.aspx
33 http://www.esecurityplanet.com/network-security/german-defense-ministry-announces-cyber-warfare-unit.html
34 http://www.oas.org/csh/ces/documentos/ce00339s02.doc

Ministros de Defensa de las Américas (2002).

- Establecer una lista de medidas para el fomento de la confianza en materia de seguridad para ser adoptadas a nivel bilateral, subregional y regional, que incluya medidas políticas, diplomáticas, educativas y culturales, militares y otras no militares, Comisión de Seguridad Hemisférica de la OEA (2003).
- Proteger la Infraestructura Crítica para salvaguardar las telecomunicaciones y redes de computadoras (2003).
- Establecer una "Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernetica" para proteger la infraestructura de las telecomunicaciones y sus redes y sistemas de información en respuesta a los ciberincidentes (2004).
- Crear de una "Red Interamericana de Seguridad Cibernética", por medio de grupos nacionales de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSRITs) para identificar y luchar contra las amenazas emergentes creando una red interamericana de vigilancia y alerta sobre seguridad cibernética (2005).
- Definir "la Infrestructura Crítica en el Hemisferio", entendida como "entre otras, en aquellas instalaciones, sistemas, y redes, así como servicios y equipos físicos y de tecnología de la información cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, la gobernabilidad democrática, o el eficaz funcionamiento del gobierno de un Estado miembro" (2007).

La ciberdefensa en Brasil

El ministro de Defensa de Brasil, Celso Amorim, y el Secretario de Defensa de Estados Unidos, Leon Panetta, se reunieronel 24 de abril de 2012 en Brasilia donde realizaron avances en la cooperación entre ambos países en materia de defensa cibernética. Al respecto, Amorín indicó que la utilización del término "guerra" es exagerado para el momento actual, ya que los alcances de la guerra cibernética son desconocidos, aunque la existencia de armas cibernéticas es perceptible, lo que presenta preocupaciones por los riesgos que representan para las redes de gobierno, en especial los ataques a informaciones protegidas y los ataques a la fragilidad de las infraestructuras críticas del Estado, como la paralización del programa nuclear iraní por el vírus Stuxnet.

Asimismo, el Ministro indicó que en 2010, el Ministerio de Defensa creó en el ámbito del Ejército el Centro de Defensa Cibernética (CDCiber) con la misión de profundizar las amenazas, establecer una doctrina nacional sobre el tema y perfeccionar los medios de defensa contra esas amenazas. Asimismo indicó que se

encuentra en análisis una política de defensa cibernética[35].

Para el comandante de este centro, el General José Carlos dos Santos, "en una situación de ataque, si usted es capaz de identificar a un atacante en la red, sería lícito neutralizar ese ataque". Para ello, el personal de este Centro ya ha tomado capacitación de ataque ofensivo, específicamente los cursos de la empresa Offensive Security. Actualmente el CDCiber cuenta con un personal de 35 militares, pero apunta a llegar a 140 en el mediano plazo. Santos indicó que el CDCiber va a necesitar de unos 45M USD por año hasta el 2015.

Dentro de esas medidas se destaca que a principios de 2012 el Ejército brasileño anunció la compra de nuevo software para seguridad y prevención contra ataques cibernéticos[36].

En tal sentido, el General Antonio Santos Guerra, director del Centro de Comunicaciones y Guerra Electrónica del Ejército (Ccomgex) que forma parte del CDCiber, expresó que: "tenemos una preparación mínima para escenarios de ataque. Tenemos un gran red, la EBnet, que reúne los cuarteles en todo el país, y está bien blindada, pero tiene puntos de vulnerabilidad"[37], resaltando que es preciso garantizar durante una crisis la infraestructura crítica de Brasil, en su mayoría a cargo de compañías privadas. En enero de 2012 las Fuerzas Armadas completaron las licitaciones para la compra de un antivirus y de un programa que simula ataques cibernéticos a ser desarrollados por empresas brasileñas. Según el general, el simulador de guerra cibernética entrenará a los oficiales en por lo menos 25 escenarios de diversos tipos de ataque contra redes semejantes a las del Ejército.

De acuerdo con el Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad (CERT), que reúne notificaciones de ataques electrónicos en todo el país, Brasil registró casi 400 mil ataques a computadoras en 2011.

La ciberseguridad en Argentina.

Argentina cuenta con un sistema nacional frente a estos desafíos. Creada en 1999, la oficina Coordinación de Emergencias en Redes Teleinformáticas (ArCERT), dependiente de la Jefatura de Gabinete de Ministros (JGM), es la unidad de respuesta (CSIRT) que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública Nacional, ante cualquier ataque o intento de penetración a través de sus redes de información[38]. ArCERT difunde información para la prevención, manejo y recuperación de incidentes, asesora y capacita a personal técnico de organismos del

35http://www.defesanet.com.br/cyberwar/noticia/5954/CDCiber---Centro-de-Defesa-Cibernetica-inicia-em-Junho

36 http://www.kungfoosion.com/2012/05/el-cdcyber-de-brasil-se-prepara-para.html

37 http://www.bbc.co.uk/mundo/noticias/2012/03/120315_brasil_guerra_cibernetica_adz.shtml

38 http://www.arcert.gov.ar

Sector Público Nacional y centraliza los reportes sobre incidentes de seguridad en el sector público para afrontarlos.

Desde el año 2003, la Oficina Nacional de Tecnologías de Información (ONTI), dependiente de la JGM, es el organismo responsable en la formulación de políticas y en la implementación del proceso de desarrollo e innovación tecnológica para la transformación y modernización del Estado, debiendo, entre otras acciones, entender en los aspectos relativos a la seguridad de la información digitalizada y electrónica del Sector Público Nacional, teniendo bajo su área Arcert. El 3 de agosto de 2005, la ONTI aprobó la "Política de Seguridad de la Información Modelo para el Sector Público"[39] la cual estableció una Política de Seguridad en cada Organismo (ISO/CEI 17799).

En 2010, la Presidenta de la Nación emitió el Decreto 1552/2010 denominado "Plan Nacional de Telecomunicaciones "ARGENTINA CONECTADA", que determina una infraestructura nacional de telecomunicación y establece ejes estratégicos. El Plan conforma una Comisión de Planificación y Coordinación Estratégica en la órbita del Ministerio de Planificación Federal, Inversión Publica y Servicios, integrada por representantes de organismos públicos nacionales. El mismo, instruye a la empresa estatal AR-SAT, a llevar adelante las acciones para la implementación de la Red Federal de Fibra Óptica y el Plan "Argentina Conectada". Como ejes estratégicos, el Plan establece 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 de la competencia. En materia de infraestructura y conectividad, el Plan establece una Red Federal de Fibra Óptica, para la inclusión digital que se divide en cuatro infraestructuras fundamentales: el Centro Nacional de Operaciones y Punto Nacional de Acceso a la Red; los Centros Provinciales de Operación y Puntos Provinciales de Acceso a la Red; la Red Troncal Federal, Red Federal de Fibra Óptica y; las Redes y anillos Provinciales.

Por su parte, en el ámbito de la Seguridad Interior, dependientes del Ministerio de Seguridad, las distintas fuerzas de seguridad cuentan con áreas específicas en materia de ciberdelitos. El cibercrimen ha desarrollado una nueva mirada criminológica [40] en virtud de nuevas conductas delictivas[41], donde la informática forense, se constituye en una herramienta para combatir la ciberdelincuencia[42].

39 http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

40 Sain, Gustavo. El fenómeno del cibercrimen en Internet y la WWW: una mirada criminológica. Cuadernos de Seguridad del Ministerio de Seguridad. N° 12. 2010. http://www.minseg.gob.ar/cuadernos/cuaderno-nro-13

41 Savaro, Carlos, Subcomisario PFA. 2° jefe de la División Delitos en Tecnologías y Análisis Criminal. Nuevas tecnologías y conductas delictivas. Idem N° 11. 2009. http://www.minseg.gob.ar/cuadernos/cuaderno-nro-11

42 Gomez, Angel. Segundo Comandante GNA. Jefe de División Seguridad Informática de GNA. La informática forense, una herramienta para combatir la ciberdelincuencia. Idem 43.

La ciberdefensa en el Sistema de Defensa Nacional

La Ley 23.554[43] de 1988 define a la Defensa Nacional como la integración y la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes. Asimismo, el Decreto 727/06, fortalece el rol del Estado Mayor Conjunto de las Fuerzas Armadas (EMC) como principal ejecutor de las decisiones estratégicas determinadas por la conducción civil y como último órgano militar encargado de ejercer las funciones de comando y organización de las fuerzas armadas. Su Jefatura VI - C3I2 (Comando, Control, Comunicaciones, Interoperabilidad e Informática) tiene como misión desarrollar y monitorear políticas, planes, programas y proyectos relacionados con los sistemas de C3I2 Conjuntos y Combinados.

A fines de 2010, en el marco del Bicentenario, el Ministerio de Defensa publicó la actualización del "Libro Blanco de la Defensa Nacional"[44], donde en materia de ciberdefensa:

- 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".
- Entiende 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.
- Determina que "estas tecnologías contribuyen al control efectivo de los espacios terrestres, marítimos y aeroespaciales de la Nación".
- Establece siete Programas Transversales Sistémicos, de los cuales en materia de "Ciberespacio", establece desarrollar:

  - "tecnologías destinadas a asegurar la confidencialidad, integridad y disponibilidad de la información esencial para mantener la continuidad operativa del ciberespacio que configura una nueva dimensión operacional –independiente y omnipresente– en los espacios terrestres, marítimos y aeroespaciales de jurisdicción e interés".

43 http://www.mindef.gov.ar/secciones/documentos/ley_23554.htm
44 http://www.mindef.gov.ar/images/banners/banner_libro-blanco.gif

"ingenios militares, capacidades, organizaciones y recursos humanos que aseguren el uso y el control del ciberespacio específico de los componentes del Sistema de Defensa Nacional, y aquellos ámbitos de interés estratégico asociados ante agresiones externas contra el ciberespacio nacional (ciberguerra)".

Dependiente del Ministerio de Defensa, el Instituto de Investigaciones Científicas y Técnicas para la defensa (CITEDEF) es un organismo centralizado y desconcentrado, dependiente de la Subsecretaría de Investigación Científica y desarrollo Tecnológico del Ministerio. Tiene responsabilidad primaria en la ejecución de los planes, programas y proyectos de investigación y desarrollo enmarcados en las políticas científico-tecnológicas para la defensa. Realiza investigación y desarrollo (I+D) en materia de comunicaciones, electrónica y defensa y seguridad informática, provee capacidades para el análisis de redes, pruebas de vulnerabilidad, configuración de servidores seguros, implementación de firma digital, configuración de firewalls, así como Proyectos de Investigación en Sistemas de Detección de Intrusiones. En el año 2004 es creado el Laboratorio de Investigación y Desarrollo en Seguridad Informática (Si6) para la Detección, Clasificación e Identificación de Intrusos, Honeypots, Análisis de Patrones, Redes Privadas Virtuales (VPN), Firewalls, Firma Digital y Penetration Tests, entre otros. Asimismo, el Programa de Investigación y Desarrollo para la Defensa (PIDDEF) del Ministerio de Defensa tiene como objetivo en el corto plazo la unificación de las actividades de investigación y desarrollo informática, *software* y *hardware* en un único centro[45].

Cabe destacar que el 17 de abril de 2012 mantuvieron un encuentro de trabajo bilateral en Brasilia los Ministros de Defensa de Argentina, Arturo Puricelli, y su par de Brasil, Celso Amorim, donde a su término, se realizó una declaración conjunta tendiente a la cooperación bilateral trabajando en el fortalecimiento de las relaciones bilaterales, con el acuerdo de los siguientes temas puntualizados en la declaración final la cual en la presente materia indica "ampliar la cooperación en materia de capacitación y adiestramiento entre escuelas militares"; impulsar iniciativas conjuntas en el campo de la industria, de la ciencia y la tecnología, incrementar la realización de ejercicios operacionales entre las FF.AA. de ambos países, fomentar la asociación entre las industrias de defensa y profundizar la cooperación en defensa cibernética"[46].

El Ejército Argentino cuenta con la Dirección General de Comunicaciones e Informática. Sus antecedentes se remontan a fines del siglo XIX y, en virtud de los avances tecnológicos y el impacto de las Tecnologías de la Información en el campo militar terrestre[47], a mediados de los años 90 se fusionan las áreas de Sistemas de Comunicaciones e Informática, con la finalidad de administrar y gestionar en forma integrada ambos en el Sistema Único de Comunicaciones (SUCOM), den-

45 Idem 32, pág 283.
46http://www.aeroespacio.com.ar/industria-y-tecnologia/item/808-argentina-y-brasil-profundizan-sus-relaciones-en-materia-de-defensa.html
47 "Ejército Argentino: su desarrollo operativo 1990-1999, una fuerza para el siglo XXI", pág. 155 a 173.

tro del cual diferentes subsistemas satisfacen las necesidades de procesamiento, transporte y gestión de información integrada, para brindar a los usuarios, apropiadas facilidades convergentes de voz y de datos[48], dependiendo de ellas las respectivas unidades.

La ciberdefensa en los estudios militares

Actualmente en la Escuela Superior Técnica[49] (EST), dependiente del Instituto Superior de Enseñanza del Ejército Argentino (IESE), se dicta la carrera de Ingeniería en Informática e Ingeniería Electrónica, de la que son cursantes civiles y militares y se especializan en aspectos que hacen a la seguridad informática mediante cursos de post-grado como "Especialista en Criptografía y Seguridad Teleinformática"[50]. Asimismo, la EST desarrolla cursos de capacitación en materia de seguridad informática y de las comunicaciones, guerra electrónica, etc. Estas capacidades también se encuentran en los institutos de formación de la Armada Argentina y en la Fuerza Aérea Argentina.

La Escuela Superior de Guerra "Tte Grl. Luis María Campos" (ESG) por medio del Departamento Juegos de Simulación desarrolla actividades en el Adiestrador Táctico (ADITAC)[51]. En este ámbito se conceptualizan, confeccionan y desarrollan ejercicios en forma integrada mediante el empleo de simulaciones bajo el concepto de Simulación Digital Interactiva (SDI) por medio del Sistema Batalla Virtual de origen y desarrollo Nacional. El empleo de sistemas de simulación entrena y adiestra a los alumnos de la ESG en el proceso de Comando y Control, en el proceso de apreciación de situación, impartición de órdenes y control de las operaciones, facilitando el uso apropiado del terreno, la gestión de información y el cálculo, proporcionando respuestas aptas a las decisiones de comando, en tiempo real y otorgando una probabilidad de aproximación a lo óptimo, brindando educación, entrenamiento y adiestramiento para la toma de decisiones.

Asimismo, Argentina es sede para América del Sur de la Asociación Internacional de Comunicaciones Electrónicas de las Fuerzas Armadas (AFCEA Internacional), organización civil que reúne a especialistas en temas de C4ISR (Comando, Control, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento).

En los últimos años, en el ámbito académico del Ejército se han desarrollado diversos estudios militares resultados de trabajos académicos sobre el tema que aportan actualizaciones conceptuales en la materia. De ellos se destacan las siguientes apreciaciones:

48 http://www.cominf.ejercito.mil.ar
49 http://www.ingenieriaest.iese.edu.ar
50 http://www.ingenieriaest.iese.edu.ar/index.php
51 http://www.escuelasuperiordeguerra.iese.edu.ar/menu/adiestrador.php

- Para alcanzar "el poder en el ciberespacio, se requiere de una Estrategia Cibernética; organizar la Fuerza Cibernética; desarrollar las armas que esa estrategia particular requiera". El espacio cibernético donde se desarrollan las "operaciones cibernéticas" amplía su radio de acción y tiempo[52].

- "El dislocamiento estratégico operacional" es una situación que se logra por medio de la aproximación directa o indirecta sobre la fuerza enemiga producto del desequilibrio de su dispositivo, desarticulación de su comando, afectación de su moral y de la capacidad de maniobra y obtención de sus líneas de menor resistencia y expectativa. Para lograrlo se requiere desarticular el comando del enemigo, desquilibrar sus fuerzas, afectar su moral y capacidad de maniobra, desorganizar sus abastecimientos y afectar sus líneas de comunicaciones. En las nuevas ciberguerras este "dislocamiento" se alcanza por medio de capacidad tecnológica, informática y digital [53].

- "Las amenazas a la infraestructura de información nacional" requieren aplicar la teoría sistémica de Warden de los "cinco anillos estratégicos" para **desarrollar un escenario de ciberguerra** atacando el "sistema de sistemas" C4ISR mantener con tecnología de la información la capacidad de comando y control. Las amenazas a la infraestructura de información nacional son muy reales, no tradicionales y altamente diversificadas por lo cual es necesario desarrollar conceptos operacionales y estructuras organizativas que les permitan, ser capaces de luchar a fin de obtener la superioridad en este nuevo ámbito y también poseer la habilidad suficiente para combatir en ese ámbito, tomando ventaja de los errores que el adversario cometa en el espacio de información[54].

- "La defensa de la información contenida en los sistemas digitales desde la paz, disminuye los riesgos en la toma de decisiones durante los períodos de crisis y conflictos armados [55].

- Los "Objetivos básicos de la Seguridad Informática militar" son: confidencialidad de la información, integridad del mensaje, confiabilidad o autenticidad y disponibilidad. Para un **escenario de ciberguerra** se necesitan profesionales que formen parte de la Gran Unidad de Combate[56].

52 Stell, Enrique. Cnl (r) VGM. Guerra Cibernética. Editorial Círculo Militar, Biblioteca del Oficial Volumen 791, Buenos Aires, 2005, pág. 17 y 27.
53 Pritz, Roberto. Grl Br (r). El Dislocamiento estratégico operacional en las nuevas guerras: IW, ciberguerra, sistemas C4I, nuevas armas y tecnologías. Escuela Superior de Guerra, 2005.
54 Cargnelutti, Hugo. Cnl (r). Conceptos sobre Guerra de Información. Revista de la Comisión del Arma de Comunicaciones. Número 27. 2002. Pag 11.
55 Machiandiarena, Tabeada y Gaidano. Mayores. Licenciatura en Estrategia y Organización (ESG-IESE). 2003.
56 Idem 56 referencia al Capitán Fabian Calvete, OIM en Informática (EST-IESE).

Conclusiones

La era de la información posee un nuevo espacio informacional y una infraestructura crítica que lo soporta, demandando esfuerzos gubernamentales. Los nuevos conflictos de esta era han dado lugar a la denominada guerra de la información, donde se intenta atacar los nudos o "nodos" de los sistemas de comunicaciones, administración, comercialización, etc. de las redes informáticas y las infraestructuras que las soportan. No se trata solamente de atacar un pozo petrolero para evitar el flujo de combustible, o como era un ataque en la transición de la era industrial a la nueva era. Se trata de atacar una central nuclear, un centro financiero, un complejo militar, un sistema de comunicaciones gubernamentales o infectar una red de computadoras, afectando así la totalidad del sistema de una nación, y ya no necesariamente en términos de guerra clásica. Por tal motivo, las estrategias nacionales, bilaterales y multilaterales en esta materia comienzan a delinear estrategias y orientar recursos para proteger las infraestructuras críticas informacionales de cada nación y región, tanto en la faz pública como privada, lo que demanda también crear capacidades y legislación específica, y, dentro de ellas en materia de defensa.

La complejidad que presenta este nuevo tipo de amenaza por la asimetría entre sus actores, multidimensionalidad de los escenarios y su, por momentos, intangibilidad dentro del nuevo ciberespacio. Asegurar las infraestructuras críticas, neutralizar las acciones en su contra y detectar a futuro otras, procurando ciberdefensas, son medidas continuas y constantes que demandan eficacia y eficiencia en su resolución.

Frente a este desafío surge el imperativo estratégico de prepararse, adiestrarse, reconfigurándose en el entendimiento de un nuevo ambiente estratégico, donde el Campo de Marte real, virtual y su soporte infraestructural, se amplia al ciberespacio, lo que da lugar a nuevas estrategias para la acción en materia la denominada defensa cibernética.

Curriculum Vitae del Doctor J. Ulises Ortiz

Doctor en Ciencia Política y graduado en Relaciones Internacionales por la Universidad del Salvador (USAL). Es Magister por la Universidad Católica de Salta (UCSalta) y Postgraduado en: "Estrategia I y II", Escuela Superior de Guerra "Tte Grl L.M. Campos".

Es Investigador - Docente Categoría II, acreditado por la Secretaría de Políticas Universitarias del Ministerio de Educación e Investigador Principal - Jefe de Proyecto (Ii C3) acreditado por la Subsecretaría de Investigación Científica y Desarrollo Tecnológico del Ministerio de Defensa.