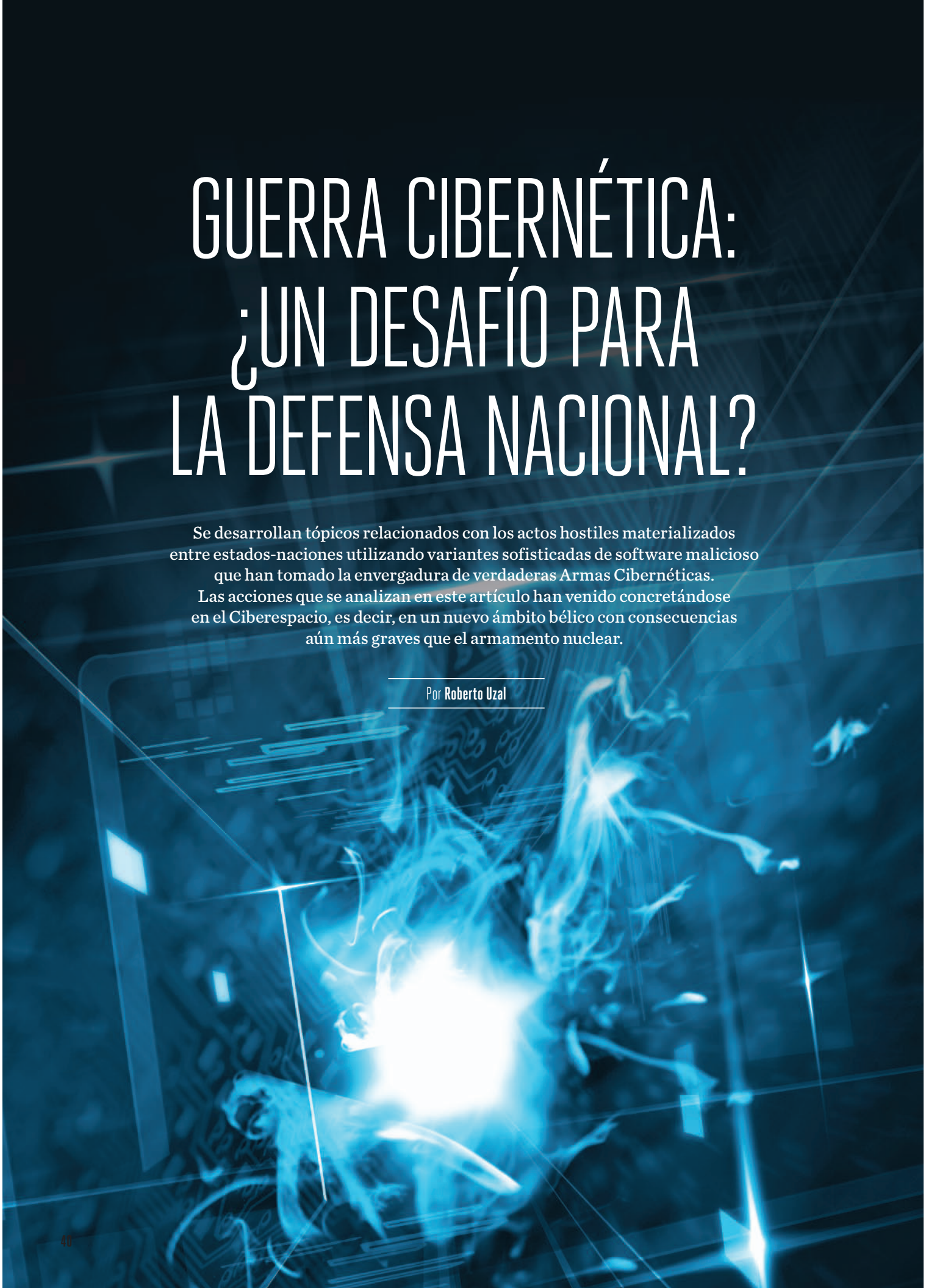
GUERRA CIBERNÉTICA: ¿UN DESAFÍO PARA LA DEFENSA NACIONAL?

Se desarrollan tópicos relacionados con los actos hostiles materializados entre estados-naciones utilizando variantes sofisticadas de software malicioso que han tomado la envergadura de verdaderas Armas Cibernéticas. Las acciones que se analizan en este artículo han venido concretándose en el Ciberespacio, es decir, en un nuevo ámbito bélico con consecuencias aún más graves que el armamento nuclear.

Por **Roberto Uzal**



INTRODUCCIÓN

La Guerra Cibernética es eminentemente asimétrica. No es un "lujo" que incumbe sólo a los países más poderosos. Paradójicamente, aquellos con Fuerzas Armadas que más han avanzado en la adopción de sistemas de Comando y Control integrados, son los que deben esforzarse en cubrir sus "flancos débiles" derivados del uso intensivo de redes teleinformáticas complejas.

Es por ello, que el vice ministro de Defensa de los Estados Unidos, William J. Lynn III, estableció claramente: *Tenemos en el Cyber Command (Comando Cibernético) un completo espectro de capacidades, pero la esencia de la estrategia es defensiva*[1]. En el mismo artículo, Lynn asevera que *Cyber Command / Cyber Space* definen un nuevo ámbito de una nueva Fuerza Armada.

Países medianamente desarrollados que adquieran las correspondientes capacidades en Guerra Cibernética, podrán lograr un importante reposicionamiento en el contexto global. De allí que Lynn III señala que la estrategia cibernética prioritaria de los Estados Unidos sea la defensiva. El número de enemigos con capacidad de causar devastación en territorio norteamericano se multiplica en un contexto de Guerra Cibernética.

Uno de las escenarios potenciales más desfavorables que se le puede presentar a un estado-nación es recibir ataques cibernéticos y, por incapacidad tecnológica y/o de gestión, terminar adjudicando los desastres ocasionados por dichos ataques a accidentes impredecibles.

No debe confundirse Guerra Cibernética con Guerra Electrónica. Los países que cometieron ese error se han posicionado con desventajas competitivas. Para aportar a que se distingan las diferencias, se hace mención al modelo de interconexión *International Standard Organization – Open Systems Interconnection* (ISO-OSI) que define siete capas conceptuales cuando dos o más computadores interactúan entre sí, a saber: capa Física, de Datos, de Red, de Transporte, de Sesión, de Presentación y de la Aplicación.

En tanto, las primitivas armas cibernéticas actuaban prioritariamente en niveles cercanos a la capa Física, las actuales son afines a capas cercanas a la de Aplicación. Ejemplo: Armas cibernéticas que modifican el funcionamiento de los "Controladores de Lógica Programable" de plantas nucleares o de plataformas de exploración petrolera.

En otras palabras, la "Guerra Electrónica" incumbe el uso de niveles de la referencia[2] cercanos a la capa Física. Se corresponde con los ámbitos "tradicionales" de los conflictos: tierra, mar y aire. La "Guerra Cibernética" se desarrolla en un nuevo ámbito de las hostilidades entre estados-naciones: El Ciberespacio.

La Guerra Cibernética no es incumbencia exclusiva de ninguna de las Fuerzas Armadas. Tampoco se corresponde con el objeto específico de las denominadas "armas o servicios", "especializaciones" o "aptitudes especiales" de las Fuerzas.

Se debería trabajar en forma conjunta, aportando los mejores recursos humanos en los temas específicamente militares del Ciberespacio, requiriendo un tratamiento eminentemente cooperativo e interdisciplinario.

GUERRA CIBERNÉTICA: ACTOS HOSTILES ENTRE ESTADOS-NACIONES

- La masiva y devastadora agresión cibernética de Rusia a aeropuertos, sistemas ferroviarios, hospitales, sistema financiero y medios periodísticos de Estonia, en el 2007, provocó la reacción de Alemania en apoyo a Estonia y, luego, la intervención de la OTAN[3,4,5]. A partir de este conflicto la OTAN, consolidó su política y estructura de Guerra Electrónica. Los gobiernos de Francia y Alemania comprobaron que miembros de las agencias de inteligencia estadounidenses trabajaban junto a los desarrollistas de los productos Microsoft y algunas agencias disponían del "código fuente" de sus productos, razón por la cual la Alianza Europea excluyó de su esquema a los Estados Unidos.
- La alteración del software de un Sistema de Radar ruso en el Norte de Siria, a orillas del Éufrates, en el 2007 impidió detectar a cazas bombarderos de Israel que atacaron y destruyeron instalaciones sirias[6].
- La intrusión de China en sistemas satelitales de los Estados Unidos [7,8].

No debe confundirse Guerra Cibernética con Guerra Electrónica. Los países que cometieron ese error se han posicionado con desventajas competitivas.

1. Karen Parrish, American Forces Press Service, Washington, July 14, 2011.
2. http://www.iso.org/iso/home/search.htm?qt=iso+osi&sort=rel&type=simple&published=on vigente actualmente (2007).
3. http://news.bbc.co.uk/2/hi/europe/6665145.stm (2007).
4. http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (2007).
5. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (2007).
6. Clarke, Richard y Robert Knake, Cyber War, Harper Collins, 2012.
7. http://www.defence.pk/forums/chinese-defence/162210-hacked-how-china-stealing-americas-business-secrets.html (2012).
8. http://www.techweekeurope.co.uk/news/chinese-hackers-blamed-for-us-satellite-attack-44102 (2011).

No contar con claras definiciones que distingan: Guerra Cibernética, Terrorismo Cibernético y Crimen Cibernético producirá un efecto "Torre de Babel" privando de la eficacia necesaria para que nuestro país cuente con las mínimas capacidades de Defensa ante potenciales agresiones cibernéticas.

- El prácticamente confirmado acceso por parte de China, a información del área Defensa altamente sensible, residente en la Intranet del *Jet Propulsion Laboratory (California Institute of Technology* – NASA) [9,10].
- La voladura, utilizando "virus de red" o "gusanos", de las baterías de centrífugas en la planta de enriquecimiento de uranio en Natanz, Irán [11,12,13].
- La presencia de la más sofisticada arma cibernética, "Flame"[14], en las plataformas de explotación petrolera de Irán [15,16].
- La Guerra Cibernética de carácter *sine die* entre Pakistán y la India hizo que estos países recurriesen a hackers "privados" llevándolos a una suerte de categoría de "Cyber Contractors" [17,18].

CRIMEN CIBERNÉTICO, TERRORISMO CIBERNÉTICO Y GUERRA CIBERNÉTICA

No contar con claras definiciones que distingan: Guerra Cibernética, Terrorismo Cibernético y Crimen Cibernético producirá un efecto "Torre de Babel" privando de la eficacia necesaria para que nuestro país cuente con las mínimas capacidades de Defensa ante potenciales agresiones cibernéticas.

Por ello, es necesario precisar:

- **Crimen Cibernético:** Acto criminal cometido mediante la utilización de computadoras como herramientas principales. En algunos casos se distingue entre acto ilegal relacionado con computadoras en el cual el computador tiene un rol ocasional y acto ilegal asistido con computadores donde el computador es esencial para cometer el delito. Para que exista crimen cibernético el computador no sólo juega un papel muy relevante sino que también deben darse profundos conocimientos informáticos por parte de quienes delinquen. Existe crimen cibernético si computadores han sido objeto, sujeto o instrumento del ilícito.
- **Terrorismo Cibernético:** La definición del FBI es: *El uso ilegal de la fuerza o violencia contra personas o propiedades para intimidar o ejercer coerción a gobiernos, población civil o, de la misma manera, a algún sector / segmento, para el logro de objetivos políticos o sociales.* Se interpreta que Ciber Terrorismo es Crimen Cibernético pero realizado por motivaciones religiosas, sociales o políticas [19,20].
- ***Cyber War:*** Según Jeffrey Carr, autor de *Inside Cyber Warfare,* sólo se da en acciones de un estado-nación contra otro estado-nación. Confundir Guerra Cibernética con Crimen Cibernético es un grave error conceptual. El robo de identidad de un usuario de tarjeta de crédito no admite el mismo tipo de tratamiento jurídico que la destrucción de plataformas de exploración petrolera de un estado-nación por parte de otro estado-nación. La intervención de organismos como Naciones Unidas es también esencialmente distinta en este caso [21].

CAMBIO DE PARADIGMA EN SEGURIDAD INFORMÁTICA

La Seguridad Informática ha pasado a ser un tema de altísima sensibilidad y de vital importancia en el área de Defensa ya que su alcance superó el ámbito de *un sistema informático, sus administradores y sus usuarios.*

Esta Seguridad implica: protección de la "grilla" eléctrica del país, aseguramiento de las prestaciones de los aeropuertos, seguridad de las destilerías de petróleo y oleoductos, continuidad del funcionamiento de los sistemas ferroviarios, confiabilidad del sistema financiero, funcionamiento de hospitales, confianza en los sistemas de comunicaciones, continuidad de los servicios satelitales y, como ya se expresó, muchos otros ámbitos esenciales en el funcionamiento de un estado-nación.

El cambio de paradigma en cuanto a Seguridad Informática obliga a que los países adquieran capacidades para:

- Impedir o al menos detectar el ingreso de programas de computadora al-

9. http://www.foxnews.com/scitech/2012/03/01/chinese-hackers-nasa-jpl-lab/ (2012).
10. http://www.examiner.com/article/chinese-cyber-specialists-hacked-into-highly-sensitive-nasa-s-jpl-lab (2012).
11. http://www.telegraph.co.uk/technology/news/9305704/Barack-Obama-ordered-Stuxnet-cyber-attack-on-Iran.html (2012).
12. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (2012).
13. http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer malware/stuxnet/index.html (2012).
14. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
15. http://timesofindia.indiatimes.com/tech/enterprise-it/security/Flame-virus-fight-began-with-oil-attack-Iran/articleshow/13683899.cms (2012).
16. http://www.dailytelegraph.com.au/news/breaking-news/flame-cyber-virus-linked-to-more-malware/story-e6freuz9-1226476199712 (2012).
17. http://www.aljazeera.com/NEWS/ASIA/2010/12/20101241373583977.html (2012).
18. http://www.thenews.com.pk/Todays-News-13-16932-India-accuses-Pakistan-of-cyber-warfare-workers-exodus (2010).
19. http://www.fbi.gov/about-us/investigate/cyber/cyber (vigente a la fecha de presentación del artículo).
20. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (vigente a la fecha de presentación del artículo).
21. Carr, Jeffrey, "Inside Cyber Warfare, O'Reilly Media, 1ra. edición, diciembre de 2009.

tamente especializados ("Gusanos", "Caballos de Troya" y "Bombas Lógicas") a las instalaciones gubernamentales más sensibles, en nuestro caso, a las relacionadas con la Defensa Nacional.

- Identificar dichos programas maliciosos, para aislarlos, confinarlos y luego reconstituir el código fuente de dichos programas mediante conceptos y técnicas de ingeniería reversa[22] o ingeniería "hacia atrás", para poder detectar la fuente emisora de dichos programas y eventualmente sus desarrolladores, constructores.
- Neutralizar la capacidad de emisión de *malware* desde las fuentes de origen.

En el ámbito del proceso de construcción de Software de Aplicación, en el contexto de la Guerra Cibernética, se deben encarar acciones creativas y efectivas para conferirle un adecuado nivel de robustez que permita rechazar o mitigar los efectos de ataques mucho más sofisticados que los virus hasta ahora conocidos.

En síntesis: Que el software sea robusto pasa a ser igualmente importante a que haga correctamente su trabajo.

Cabe mencionar, como ejemplo de esquema defensivo, al "Escudo Dorado" *(Golden Shield)* conocido, también, como el "Gran Cortafuegos de China" *(Great Firewall of China)*[23, 24].

En un principio, fuentes occidentales catalogaron al "Escudo Dorado" como un gigantesco sistema informático dedicado, prioritariamente, a la censura de toda la información que entrara o saliera de China a través de Internet. Hoy se reconoce a este país como el mejor preparado para resistir ataques cibernéticos. China ha sido el primer país que detectó el cambio de paradigma en Seguridad Informática y, por ende, actuó en consecuencia.

Como casi todo lo que se hace en China, el resultado logrado por el "Escudo Dorado" fue notable. Su construcción se inició en 1998 y se invirtieron 800 millones de dólares. Entró en servicio en el 2003 completando su total funcionamiento en el 2008. Alrededor de 30.000 técnicos y funcionarios constituyeron la dotación de recursos humanos para desarrollarlo, implantarlo y ahora para mantenerlo actualizado.

Una cuestión fundamental: la experiencia acumulada a la fecha muestra claramente que, en el nuevo contexto de confrontación entre países utilizando Armas Cibernéticas sumamente sofisticadas, resulta estrictamente necesario que se conformen bloques o alianzas político / tecnológicas. Este sistema de alianzas, en el ámbito de la denominada Guerra Cibernética, ha sido necesario, inclusive, para los Estados Unidos de América.

Las agresiones que se han verificando entre estados-naciones, utilizando una nueva generación de armamento basada en sofisticados programas de computadoras, obligan a repensar las relaciones internacionales y a redefinir las incumbencias de lo que conceptual e instrumentalmente se entiende como Defensa Nacional.

Está probado que gran parte de las armas cibernéticas no son "gusanos" o "worms" que se desplazan autónomamente por las redes de computadoras. La mayoría está compuesta por "bombas lógicas" o "caballos de Troya" que estados-naciones "plantan", en "tiem-

22. Ingeniería reversa: Algunos grupos de investigación han logrado "desandar el camino". Partiendo de programas en código ejecutable, que es lo que "se encuentra" en las computadoras "infectadas", llegar a lo que los programadores habían originalmente codificado en algunos de los muchos lenguajes de programación disponibles.
23. http://www.forbes.com/2007/07/30/china-cybercrime-war-tech-cx_ag_0730internet.html (2007).
24. http://books.google.com.ar/books/about/China_s_Golden_Shield.html?id=S9rPOA2q14UC&redir_esc=y (2001).

po de paz", en Sistemas de Información de otros países.

Al respecto, Richard Clarke, miembro del Consejo Nacional de Seguridad de los Estados Unidos, expresó: *En décadas, cuando los historiadores analicen los incidentes de la Guerra Cibernética, por comparación citarán a la Guerra Fría como un período de gran transparencia, lealtad y juego limpio en la relación entre estados-naciones.*

Luego de la voladura de su planta de enriquecimiento de uranio en Natanz, Irán, muy rápidamente reforzó a "Maher", su equipo de Seguridad Informática orientado a las emergencias cibernéticas[25]. Pasaron a trabajar para el gobierno iraní desde convictos encarcelados por clonar tarjetas de crédito hasta técnicos y gerentes de empresas de tecnología informática internacionales con sede en Irán.

"Maher", el 28 de mayo de 2012, detectó, en plataformas de exploración petrolera iraníes, la presencia de un arma cibernética a la que luego se llamó *Flame*[26]. Con la ayuda de Rusia dicha arma cibernética fue reconocida y confinada de manera de poder iniciarse la ingeniería reversa.

A requerimiento de Irán, la agencia de la ONU, encargada de ayudar a los estados miembros a asegurar sus infraestructuras nacionales, emitió una enfática advertencia acerca del riesgo del virus "Flame". *Es la advertencia más seria que hemos emitido, es una peligrosa herramienta de espionaje que también podría ser usada para atacar infraestructuras críticas*[27, 28, 29], dijo Marco Obiso, coordinador de Ciber Seguridad de la Unión Internacional de Telecomunicaciones de la ONU.

La evidencia sugiere que "Flame" podría haber sido desarrollado por el mismo país o países responsables del gusano "Stuxnet", casualmente el virus que atacó, en el 2010, a una de las plantas vinculadas al programa nuclear de Irán. *Creo que es mucho más serio que el Stuxnet,* dijo Obiso. De hecho estaría probado que el código fuente de "Stuxnet" habría sido "reutilizado" en "Flame". Todo esto no podría haber sido averiguado y difundido sin la intervención de Naciones Unidas.

Fue Kaspersky Lab[30], una empresa rusa de seguridad informática, la que identificó plenamente a "Flame" luego de que la ONU requiriera investigar los reclamos de Irán. El trabajo de Kaspersky no habría tenido trascendencia sin el soporte legal e institucional de la ONU.

Ali Abasneyad[31], director de la firma de seguridad informática iraní Kahkeshan Nur, describió a los periodistas la complejidad y el poder del arma cibernética "Flame", *la cual no tiene antecedentes. Puede requerir los servicios de otros software maliciosos preexistentres.*

Esto se denomina *dynamic binding* (enlace dinámico) en la jerga informática. Continuó Abasneyad destacando que "Flame" puede cambiar y/o ampliar sus capacidades logrando distintos resultados y/o respuestas a sus estímulos. Esta capacidad, a su vez, se denomina *polymorphism* (polimorfismo) en el contexto de la Tecnología Informática.

El técnico iraní agregó que *Flame posee inteligencia propia para localizar objetivos y determinar prioridades de ataque. Ante la oportunidad de ejecutar acciones que impliquen graves daños a un blanco, Flame pide autorización a sus C&C Servers (Servidores de Comando y Control) a los que está subordinado.*

Resulta particularmente interesante la entrevista que la televisión oficial de Irán realizó al hacker arrepentido, devenido en empresario de PyME, Behruz Kamalian[32]. El ahora directivo de la empresa Ashiané de servicios de

Desarrollar y utilizar efectivamente nuevos enfoques de seguridad en el diseño, la adquisición y construcción de Sistemas de Información sensibles para el área Defensa.

Seguridad Informática, afirmó que la prioridad de "Flame", hasta ahora, ha sido la de ocasionar daños en la industria petrolera de Irán. Asimismo, destacó *las treinta funciones específicas de Flame las que se multiplican, como se anticipó, por sus capacidades de polimorfismo y enlace dinámico.*

Mohamad Mehdi Shobeiri[33], experto en Seguridad Informática y directivo de PANDA (software antivirus)[34, 35] en Irán, explicó la capacidad de *dynamic binding* de "Flame", agregando que *se comporta como un Panel de Control de muchos otros virus y se adapta a nuevos objetivos de acuerdo a las directivas que reciba de su Servidor de C&C*[36].

Según Shobeiri, "Flame" es una herramienta de espionaje casi perfecta, transmite a su Servidor C&C lo captado subrepticiamente a través de la web cam y del micrófono de las computadoras infectadas, detecta contraseñas, roba los contactos de los celulares que estén cerca de las computadoras infectadas y retransmite los emails recibidos o enviados.

Alexander Gostev[37], investigador de la empresa rusa Kaspersky Lab, quien trabajó en la ingeniería reversa de "Flame", expresó, también a la televisión iraní, *que no es posible construir algo como Flame si no se cuenta con el respaldo de un país.*

Por otro lado, el periodista David Sanger, una suerte de Bob Woodward / Carl Bernstein de la Guerra Cibernética[38], el 1 de junio de 2012, a través del *New York Times*, reveló la alianza estratégica de los Estados Unidos-Israel en el ámbito de la Guerra Cibernética y las órdenes de ataques a Irán impartidas por el presidente Obama.

La Seguridad Informática tiene también su componente jurídico – institucional. Al respecto conviene citar a Nemat Ahmadi[39], conocido abogado iraní, que ha estudiado el "lado jurídico" de los ataques cibernéticos que ha recibido su país:

A La destrucción de la planta de enriquecimiento de uranio de Natanz.

B El abortado ataque a las plataformas de exploración petrolera iraníes.

Ahmadi, entrevistado este año por la televisión oficial iraní, expresó *que regulaciones para evitar la proliferación de guerras cibernéticas son aún más necesarias que las destinadas a evitar la proliferación de armas nucleares.* En la mencionada entrevista, el citado jurista reconoció, muy elípticamente, la muerte de científicos iraníes cuando fue destruida, en el 2010, la planta de enriquecimiento de uranio de Natanz por el arma cibernética "Stuxnet". Enfatizando, además, que Irán *tiene el derecho de responder si vuelve a ser atacado cibernéticamente.*

Estudiosos del Derecho de los Estados Unidos, sostienen *que existe jurisprudencia avalando que se considere a determinados Ataques Cibernéticos como una agresión armada a territorio estadounidense*[40, 41]. *Cyber War Law* es ya una relevante especialización del Derecho en este país del Norte.

En el mismo país, luego de que *Cyber Warriors* presuntamente chinos, en marzo de este año, accedieran a la información más sensible de la NASA, residente en la Intranet del *Jet Propulsion Laboratory* (Pasadena – California), el tema del espionaje utilizando armas cibernéticas despertó una gran polémica[42]. Existen fundamentos que señalan que, en el caso de ser aprehendidos *Cyber Intruders* que accedan a información sensible a la seguridad de los Estados Unidos, podrían quedar comprendidos en la Ley Patriótica (*Patriot Act,* 2001 renovada en el 2005) y hasta se les podría aplicar la pena capital.

Al respecto, la doctora Narges Ghoreishi[43], experta iraní en Derecho Internacional, señala que existe jurisprudencia en los Estados Unidos que permite considerar a los ataques cibernéticos como equivalentes a la invasión del territorio norteamericano, violando las Leyes de la Guerra, es decir, un Ataque Cibernético es considerado, en principio, "un crimen de guerra" según la interpretación de la Doctora.

John McCain, senador Republicano de los Estados Unidos[44, 45], criticó al presidente Obama por dejar filtrar información sobre "Stuxnet" a través de la prensa y, también, lo culpó por sus

25. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
26. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
27. http://www.itu.int/osg/spu/tnt/speaker bios.html.
28. http://www.aljazeera.com/category/person/marco-obiso (2012).
29. http://www.washingtontimes.com/topics/marco-obiso/ (2012).
30. http://latam.kaspersky.com/?sitepref=argentina&domain=kaspersky.com (vigente a la fecha de presentación del artículo).
31. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
32. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
33. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
34. www.pandasecurity.com (vigente a la fecha de presentación del artículo).
35. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
36. http://answers.yahoo.com/question/index?qid=20110910153630AA4TG4u ver "Best Answer" respecto de Servidores de Comando y Control al que "consultan" las Armas Cibernéticas sofisticadas ante situaciones críticas. Se incluye como referencia lo vigente a la fecha de elaboración del artículo, 2012.
37. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
38. Bob Woodward / Carl Bernstein: Míticos periodistas del "Washington Post" cuyos artículos, en el contexto del Caso Watergate, influyeron decisivamente en la caída del presidente Nixon.
39. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
40. http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3240/US-cyberwar-law.aspx (2012).
41. http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf (2012).

En décadas, cuando los historiadores analicen los incidentes de la Guerra Cibernética, por comparación citarán a la Guerra Fría como un período de gran transparencia, lealtad y juego limpio en la relación entre estados-naciones. ***Richard Clarke***

debilidades ante agresiones con armas cibernéticas. Indirectamente, McCain, ratificó que su país está fuertemente vinculado al desarrollo y utilización de "Stuxnet". Lo expresado por el Senador fue complementado por Michael V. Heyden, ex titular de la CIA[46], al decir que con *Stuxnet es la primera vez que se usa un virus para causar daños físicos;* siguió Heyden destacando que *Flame está en un nivel superior como arma cibernética.*

FORMACIÓN DE RECURSOS HUMANOS PARA LA GUERRA CIBERNÉTICA

Con respecto a esta formación se citan, exclusivamente, aspectos que le constan al autor en forma directa.

En el ámbito nacional, los estudios de Doctorado en Ingeniería Informática y de las Maestrías en Ingeniería de Software y en Calidad del Software, la "ingeniería reversa" es un tema altamente prioritario.

Los aspectos conceptuales e instrumentales de Auditoría Informática son de habitual tratamiento tanto a nivel grado como posgrado. La Auditoría Informática es otro aspecto muy sensible en un contexto de Guerra Cibernética.

Con respecto a la formación en las Fuerza Armadas, será necesario, en el futuro, capacitar a personal para enfrentar esta situación. Si en un corto lapso se cuenta con recursos humanos idóneos, nuestro país se posicionaría ventajosamente en el contexto internacional.

Para ello, es menester analizar la factibilidad de incorporar aspectos relativos a la Guerra Cibernética en los programas educativos.

VENTAJAS DEL POTENCIAL ESTABLECIMIENTO DE ALIANZAS REGIONALES

Este punto se desarrolla tomando como ejemplo el caso de Brasil por las siguientes razones:

- Existe, entre la Argentina y Brasil, una experiencia de décadas de trabajos mancomunados en el ámbito de la Tecnología Informática. Por el contrario de lo ocurrido en otros ámbitos, la brecha existente, a favor de Brasil, en cuanto a desarrollo en el ámbito de la Informática, se ha acortado a través de los años. Hoy casi ha desaparecido.
- Existe actualmente un provechoso intercambio con Brasil en el ámbito de la Tecnología Informática sobre todo en actividades de investigación y en el de la enseñanza de cuarto nivel[47].
- Se tiene conocimiento de actividades realizadas por Brasil en el ámbito de Guerra Cibernética.

En diciembre del 2010, el Ministerio de Defensa de Brasil, por expresa disposición del Poder Ejecutivo, creó el Centro de Defensa Cibernética (CDCiber)[48, 49]. Inicialmente está bajo la responsabilidad del Ejército Brasileño aunque su incumbencia incluye coordinar las acciones de "Defensa Virtual" para toda el área de Defensa.

Brasil ha aclarado oficialmente que el CDCiber de ninguna manera es eminentemente defensivo. El comandante de CDCiber, general José Carlos dos Santos, expresó: *en una situación de ataque, si usted es capaz de identificar a un atacante en la red, sería lícito neutralizar ese ataque.* El personal, integrante del Centro, está preparado para realizar acciones de carácter ofensivo protegiendo los intereses del Estado Brasileño y los de sus ciudadanos.

Otro antecedente importante lo constituye *The Brazilian Journal of Information Security and Cryptography*[50, 51], publicación técnico-científica de temas de Tecnología Informática de interés para el Ministerio de Defensa y el Ejército de Brasil, instituciones auspiciantes. El propósito de *Enigma,* publicación del Ministerio de Defensa de Brasil, es crear un ámbito de discusión e intercambio de información académica de temas relacionados con Guerra Cibernética.

PROPUESTAS PARA LA GESTIÓN EN NUESTRO PAÍS

- Sería importante que las más altas autoridades comiencen, si es que no lo han hecho ya, el análisis de riesgo de un ataque cibernético. Ello implica realizar una valorización de la probabilidad de ocurrencia de un ataque a instalaciones sensibles de nuestro país y determinar el costo de las acciones de prevención y mitigación frente al impacto negativo de un ataque exitoso.
- Se considera atinente se definan o redefinan las políticas de acceso a Siste-

42. http://www.washingtonpost.com/wp-yn/content/article/2011/02/15/AR2011021505395.html (2011).
43. http://www.youtube.com/watch?v=vrRj-kRofRg (2012).
44. http://www.israelnationalnews.com/News/News.aspx/156501 (2011).
45. http://www.presstv.ir/detail/2012/06/02/244298/mccain-slams-obama-govt-over-cyber-leaks (2011).
46. http://www.youtube.com/watch?v=8HK3XPXBbNk (2012).
47. http://noticias.unsl.edu.ar/2010 06 01 archive.html (2012).
48. http://www.defesanet.com.br/cyberwar/noticia/5954/CDCiber---Centro-de-Defesa-Cibernetica-inicia-em-Junho- (2012).
49. http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/ (2012).
50. http://www.egov.ufsc.br/portal/conteudo/enigma-%E2%80%93-brazilian-journal-information-security-and-cryptography (2012).
51. http://www.enigmajournal.org/ (2012).
52. C4ISR: sigla en inglés y "universal" correspondiente a "Comando, Control, Comunicaciones, Informática, Inteligencia, Vigilancia (S) y Reconocimiento" La "cuarta C" es Computer españolizada como Informática.

mas de Información que se consideren críticos para el área de Defensa.
- Se deberán definir nuevos enfoques y herramientas innovadoras tanto en la auditoría interna como en la externa de los sistemas de información más sensible a los ataques cibernéticos. Asimismo, será menester enfocar las contingencias de los sistemas de alta sensibilidad en el área de Defensa como, también, apoyar las investigaciones para detectar fuentes de orígenes de un ataque y desarrollar capacidades para neutralizarlos.
- Será necesario adoptar un concepto de "control", tal como está definido en los estándares internacionales, más efectivo y analizar la factibilidad de establecer contactos con centros de investigación universitarios que estén abocados a estos estudios.

DESAFÍOS EN EL ÁMBITO TECNOLÓGICO

- Desarrollar y utilizar efectivamente nuevos enfoques de seguridad en el diseño, la adquisición y construcción de Sistemas de Información sensibles para el área de Defensa.
- Revisar los criterios de selección del software de base utilizado en el área de Defensa y estudiar su complementación en los aspectos sensibles a la seguridad.
- Generar la capacidad de desarrollo y/o complementación de herramientas "anti-malware" de muy alta efectividad.
- Replantear el concepto y los aspectos operativos de *firewalls*. Analizar la viabilidad de la construcción de un "Escudo Dorado Brasileño – Argentino".
- Desarrollar, productos de encriptado propios, de alta confiabilidad.
- Desarrollar conceptos y herramientas propias, de detección de intrusiones a nivel país, Internet Service Providers (ISP) e Intranet de las organizaciones gubernamentales.

CONCLUSIONES Y PROPUESTAS

1. Es necesario adquirir, como mínimo, capacidades para impedir o al menos mitigar agresiones de ese tipo. Una de las situaciones más desfavorables por las que puede pasar un país es la de recibir Ataques Cibernéticos y, por incapacidad Tecnológica, terminar adjudicando los desastres ocasionados por dichos ataques a accidentes impredecibles.
2. Crimen Cibernético y Terrorismo Cibernético no son "extrapolables" a Guerra Cibernética; ni en su naturaleza, ni en lo tecnológico, ni en los aspectos legales / institucionales ni en el "gerenciamiento" / liderazgo ni en las potenciales consecuencias. Los aspectos de la Guerra Cibernética deben ser encarados con criterio de Defensa Nacional.
3. Guerra Cibernética consiste en adquirir capacidad de defensa ante agresiones que pueden ser más graves que un ataque nuclear al territorio nacional y la posibilidad de poder "neutralizar" la fuente emisora de dichas agresiones.
4. Se ratifica la paradoja de que, técnicas, enfoques o equipos correspondientes a esquemas C4ISR[52] o similares constituyen importantes vulnerabilidades en un entorno de Guerra Cibernética.
5. La Guerra Cibernética es eminentemente asimétrica. Un equipo formado por unos pocos profesionales de muy alto nivel de un estado-nación puede poner en serios problemas a sofisticadas unidades o instalaciones de otro estado-nación mucho más poderoso.
6. Se deberían definir claramente las "reglas de involucramiento" de los recursos asignados a la Guerra Cibernética. La "distancia" desde las máximas Autoridades Políticas hasta los responsables de las unidades de Guerra Cibernética debe ser la mínima posible. Decisiones sumamente trascendentes deberán tomarse casi "en tiempo real".
7. No contar con recursos aptos para la Guerra Cibernética no asegura no ser sujetos pasivos de Ataques Cibernéticos. Ocurre casualmente todo lo contrario.
8. Generar Recursos Humanos aptos para la Guerra Cibernética, a nivel de "gerenciamiento," es "la cuestión prioritaria".
9. Una alianza estratégica con Brasil para mantener el control de Ciberespacio a nivel regional sería un excelente logro; el cometido de dicha alianza sería:
   - A Mantener un control tal que evite o minimice la probabilidad de Ataques Cibernéticos a la Región.
   - B Evitar que se utilice a la Región (Argentina y/o Brasil) como "lugar de lanzamiento" de Ataques Cibernéticos por parte de "terceros" estados-naciones.
   - C Desarrollar una capacidad de "neutralización" de las eventuales "fuentes" de Ataques Cibernéticos.
10. Guerra Cibernética debería ser un tema de permanente estudio, reflexión y propuestas representando el mayor desafío a ser encarado por el área de Defensa.

Roberto Uzal
Es teniente coronel de Infantería (R), ingeniero militar (Químico – Escuela Superior Técnica) y doctor en Administración (FCE-UB). Especialista en Administración Financiera (FCE-UBA); Advanced Management Studies Certificate – pos MBA (California State University); licenciado en Sistemas (FI-UBA); investigador superior (Ingeniería) en el contexto del Programa de Incentivo a la Investigación en Universidades Nacionales. Docente universitario de grado y posgrado en la UBA. Organizador, director y profesor de la Maestría en Ingeniería de Software de la Universidad Nacional de San Luis. Autor de numerosas publicaciones científicas a nivel internacional y presentaciones en congresos y jornadas.