

La Guerra Cibernética Palestina-Israelí

Coronel Patrick D.Allen, Componente de Reserva del Ejército de los EE.UU., y
Teniente Coronel Chris Demchak, Ejército de los EE.UU.

La guerra cibernética es la guerra pionera—un combate que se conduce en una dimensión electrónica etérea de ceros y unos. El coronel Patrick D. Allen y el teniente coronel Chris C. Demchak establecen una crónica de las recientes batallas cibernéticas y discuten las medidas que los EE.UU. pueden tomar para ser victoriosos en el espacio cibernético.

El asalto actual de los ataques cibernéticos en contra de los sitios electrónicos israelíes más importantes es tal vez el más extensivo, coordinado y malicioso pirateo electrónico en la historia.

—Peggy Weigle, Directora de Sanctum Inc.¹

Esto es sólo un pequeño sabor de algo por venir.

—James Adams, Director Ejecutivo de iDefense.²

EN SEPTIEMBRE del año 2000, unos *hackers*, o piratas cibernéticos, adolescentes israelíes crearon un sitio electrónico para interferir u obstruir los sitios electrónicos de Hizbolá y Hamás en el Líbano. Los adolescentes iniciaron un constante ataque negando el servicio e interfiriendo efectivamente seis sitios cibernéticos pertenecientes a las organizaciones anteriormente mencionadas en el Líbano y de la Autoridad Nacional Palestina. Este ataque aparentemente de menor importancia dio inicio a una guerra cibernética que rápidamente se intensificó al nivel de un incidente internacional. Los palestinos y otras organizaciones islámicas llamaron para una Guerra Sagrada cibernética, denominada también un *ciber-Jihad* o *e-Jihad*.³ Inmediatamente después, los *hackers* afectaron tres notorios sitios cibernéticos israelíes que pertenecían al Parlamento Israelí (el *Knesset*), el Ministerio del Exterior y un sitio israelí de información acerca de la Fuerza de Defensa.⁴ Más tarde, los *hackers* atacaron la Oficina del Primer Ministro Israelí, el Banco

de Israel así como la Bolsa de Valores de Tel Aviv.⁵

Aunque los efectos a largo plazo de la guerra cibernética Palestina-Israelí son relativamente de menor importancia y nunca causaron una seria amenaza física a cualquiera de las naciones involucradas, los elementos del conflicto son significativos debido a que sirven como modelo para futuros conflictos cibernéticos.

La escaramuza cibernética entre EE.UU. y China en mayo de 2001 tuvo aspectos similares al incidente entre los palestinos e israelíes. Hoy en día uno se olvida que durante el ataque los *hackers* casi afectaron severamente las transmisiones de electricidad en el estado de California.⁶ Si hubiesen tenido éxito, el costo que hubiese causado a los residentes de California y al prestigio y seguridad de los EE.UU. es difícil de estimar. Los *hackers* chinos penetraron exitosamente una red de pruebas de una compañía de transmisión de poder eléctrico en California.⁷ Las lecciones provenientes de estos conflictos cibernéticos deben ser aprendidas para poder apropiadamente comprender y estar preparados para el inevitable componente cibernético de los conflictos futuros.

El Ciclo del Conflicto Cibernético

El conflicto entre *hackers* palestino-israelíes comenzó en 1999, pero dramáticamente se acrecentó luego de los problemas sociales del 28 de septiembre del año 2000. A fines de enero de 2001, el conflicto había afectado a

más de 160 sitios israelíes y a unos 35 sitios palestinos, incluyendo por lo menos un sitio estadounidense. A partir de julio de 1999 a mediados de abril de 2002, 548 sitios del dominio electrónico israelí (.il) fueron desfigurados de entre 1.295 desfiguraciones en la región del Medio Oriente, y otros sitios fueron sujetos a obstrucciones severas a sus servicios.⁸

Los dos tipos principales de ataques consistieron en desfiguraciones de los sitios cibernéticos y negación distributiva de servicio (DDoS). Las desfiguraciones de

La guerra cibernética se intensifica horizontalmente y más rápidamente que en la guerra común o estándar debido a tres razones. En primer lugar, el criterio principal para que existan ataques por parte de hackers civiles es la vulnerabilidad y no el estado crítico del blanco. La búsqueda de blancos vulnerables se amplía hasta que se encuentra uno. Si los sitios cibernéticos gubernamentales o comerciales en la nación que es el objetivo no son suficientemente vulnerables, los sitios que pertenecen a naciones amigas a la nación que se desea atacar cibernéticamente, a su vez se convierten en blancos..

los sitios electrónicos tienden a enfocarse en sitios electrónicos políticos de alta relevancia, tales como los sitios gubernamentales. En algunos casos, las transacciones comerciales fueron afectadas durante días debido a desfiguraciones constantes de sitios electrónicos.⁹ Los servidores de los sitios electrónicos que fueron empleados por los *hackers* de un lado para iniciar ataques fueron empleados a menudo por los *hackers* del lado opuesto para iniciar ataques parecidos.¹⁰ Los códigos empleados por un lado eran vueltos a ser escritos por el lado opuesto, que a su vez iniciaba un contraataque.¹¹ Los ataques empleando el método DDoS clausuró los sitios electrónicos del lado opuesto por varios días y agregó más estrés a la infraestructura del Internet en la región.¹²

Los ataques además fueron iniciados en contra de compañías provistas de infraestructura de telecomunicaciones tales como AT&T, que aparentemente fue contratada para ayudar a incrementar el ancho de banda de los sitios electrónicos israelíes que eran los blancos.¹³ El *hacker* simpatizante de los palestinos conocido como Dodi desfiguró un proveedor de servicio de Internet (ISP) que proporcionaba servicios a los ciudadanos israelíes de mayor edad y dejó un mensaje afirmando categóricamente que él podía cerrar el ISP israelí NetVision,

que es huésped de casi 70 por ciento del tráfico de la red en Israel.¹⁴

Aproximadamente el 8 de noviembre de 2001, *Unity*, un grupo extremista musulmán con lazos con Hizbolá, anunció que había iniciado la tercera fase de una estrategia consistente en cuatro fases. La primera fase enfocaba en afectar seriamente los sitios electrónicos del gobierno israelí. La segunda fase incluía ataques al Banco de Israel y la bolsa de valores de Tel Aviv. La tercera fase comprendía objetivos tales como la infraestructura del ISP israelí y el sitio para *Lucent* y *Golden Lines*, un proveedor israelí de telecomunicaciones. *Unity* reclamó que no avanzaría a la cuarta fase o fase final, específicamente la destrucción de sitios israelíes de e-comercio, amenazando así millones de dólares en pérdidas transaccionales.¹⁵

El Internet Clandestino Israelí (IIU), un grupo de *hackers* que se unieron para ayudar a incrementar la seguridad de los sitios cibernéticos israelíes, reclama que ya existen pruebas fehacientes de ataques de la cuarta fase. Esto incluye la destrucción de sitios comerciales con capacidades de e-comercio, lo cual de acuerdo al IIU causó una caída del ocho por ciento en la bolsa de valores israelí.¹⁶

A pesar de que la piratería cibernética esporádica ha existido entre los *hackers* estadounidenses y chinos en los últimos años, el choque de la aeronave de exploración estadounidense EP-3 con el interceptor chino F-8 fue el que inició el conflicto principal. Los *hackers* chinos acrecentaron sus actividades en contra de los EE.UU. e intentaron organizar un esfuerzo mayor de piratería cibernética a gran escala durante la primera semana de mayo del 2001.¹⁷

De igual manera que los palestinos, los chinos crearon un sitio cibernético del cual *hackers* voluntarios podrían obtener los instrumentos y técnicas necesarios para propulsar un programa denominado “USA Kill” (EE.UU. Matar).¹⁸ El Centro de Protección de Infraestructura Nacional de los EE.UU. anunció una alerta el 26 de abril de 2001 a todos los sitios cibernéticos del gobierno de los EE.UU. así como a todos los sitios comerciales.¹⁹ Mientras tanto, *hackers* estadounidenses provocados por el deteni-miento prolongado de la tripulación del EP-3 en China, comenzaron a organizar el programa “China Killer” (Asesino de China).²⁰ Cuando los *hackers* chinos declararon una tregua, declararon que habían desfigurado o negado servicio a más de 1000 sitios cibernéticos estadounidenses. Los *hackers* en favor de los EE.UU. aparentemente causaron el mismo nivel de daño a los sitios chinos.

Cuatro Fases de Futuros Conflictos Cibernéticos

Los conflictos cibernéticos:

- Involucrarán un período inicial de sorpresa, seguido por un período más prolongado de adaptación y recuperación.
- Se intensificarán rápidamente y ampliarán sus

efectos a medida que los atacantes buscan hallar objetivos vulnerables.

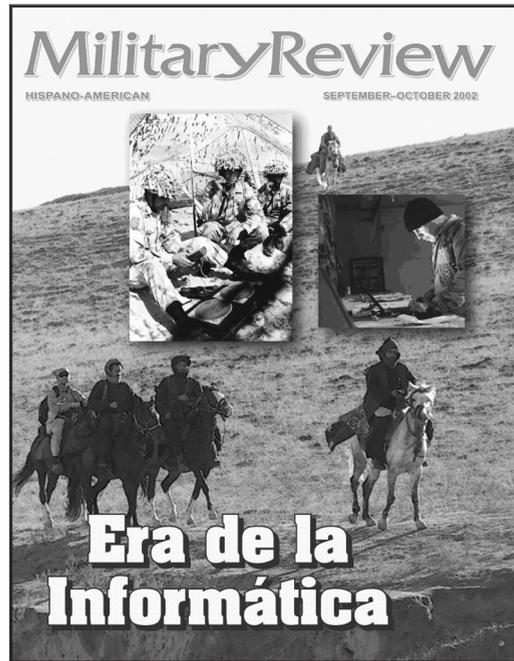
- Se desarrollarán rápidamente en conflictos internacionales a medida que los *hackers* voluntarios se alinean con o en contra de, las distintas facciones.

- Aumentarán el paso del desarrollo de armas cibernéticas y subsecuente proliferación.

Basado en observaciones de los conflictos entre Palestina e Israel y de China y los EE.UU., creemos que el futuro conflicto cibernético se desenvolverá en cuatro fases.

Fase 1: Sorpresa y Adaptación. La guerra cibernética palestina-israelí es un ejemplo excelente de cómo una nación puede ser sorprendida por un ataque cibernético. Los *hackers* adolescentes israelíes inicialmente sorprendieron a los sitios electrónicos que apoyaban la causa palestina con sus ataques empleando el método *DDoS*. Cuando los palestinos declararon un *ciber-Jihad* en contra de Israel los *hackers* a favor de Palestina alcanzaron un nivel comparable de sorpresa en contra de los sitios electrónicos israelíes que habían sido seleccionados como blancos. Los israelíes se sorprendieron que sus propios ciudadanos habían iniciado el conflicto cibernético. También se sorprendieron por la magnitud de la respuesta a favor de los palestinos y por la vulnerabilidad de sus sitios cibernéticos gubernamentales así como de los comerciales. Después del *shock* inicial, cada lado sufrió un período de reparar los daños al sistema y mejorar las defensas en contra de ataques futuros.

Vale la pena considerar los efectos iniciales del conflicto. *Jerusalem.com*, el proveedor cibernético de libros más importante en Israel, tuvo que clausurar sus actividades durante días debido a un ataque de desfiguración de la red. La compañía enfrentó varios días de pérdida de ventas y el riesgo de una prolongada desconfianza por parte de sus clientes referente a la seguridad de las transacciones vía la red.²¹ De igual manera, el sitio cibernético de la Oficina de Administración de Tierra de Israel tuvo que permanecer cerrado durante meses.²² Para Israel en general, tales cierres crearon una carencia de confianza. Además, la gran cantidad de ataques *DDoS* (más de 115 en la región entre el 6 de octubre y el 2 de diciembre de 2000) causó un tremendo estrés en la ya delicada infraestructura del Internet en el Medio Este.²³



El costo mayor del ataque cibernético es generalmente mayor para los blancos comerciales que el de los sitios gubernamentales. Como lo declaró Lawrence Gershwin, el asesor de tecnología con más jerarquía de la CIA, en un testimonio prestado ante el congreso, “Nuestra sociedad conectada vía cables nos pone a todos —los negocios estadounidenses, en particular porque deben mantener un intercambio abierto con los clientes— a un nivel de riesgo elevado con respecto a los enemigos.”²⁴

Cuando un sitio gubernamental cae o es desfigurado, la nación tal vez pierda parte de su rostro. No obstante cuando un sitio electrónico de una compañía es clausurado,

pierde lucro. Matt Krantz y Edward Iwata constataron en un artículo publicado por el periódico *USA Today* “Algunos negocios pierden US\$10.000 hasta varios millones de dólares por minuto cuando sus sitios se clausuran. . . Pierden un promedio de US\$100.000 por hora de pérdida en productividad.”²⁵ La compañía de investigación *Reality Research* evaluó que los negocios alrededor del mundo podrían haber perdido más de US\$1.5 trillón de dólares el año pasado como consecuencia de los asaltos cibernéticos.²⁶

A pesar de que los sitios comerciales tienen interés en defenderse en contra de ataques cibernéticos, el deseo de ser más efectivo con respecto al costo hace que la mayoría de las compañías ignoren las vulnerabilidades de la red hasta que son víctimas de un ataque de los *hackers*.²⁷ Por lo tanto, existe una necesidad de crear incentivos mayores para los negocios para ser más seguros en el espacio cibernético, y deberían existir penalidades si no están asegurados en una fecha determinada.

Fase 2: Rápida Intensificación Horizontal. El conflicto cibernético palestino-israelí se amplió rápidamente. En las primeras cuatro semanas del conflicto *hackers* a favor de los palestinos afectaron un sitio cibernético estadounidense. Tres semanas más tarde, *hackers* israelíes atacaron sitios cibernéticos en Irán y el Líbano.²⁸ Debido a que Israel tenía más sitios cibernéticos comparados a los palestinos desde los cuales se podía iniciar contraataques cibernéticos, los *hackers* israelíes comenzaron a buscar sitios vulnerables fuera de la Autoridad Nacional Palestina y el Líbano. Un grupo de *hackers* israelí, por ejemplo, denominándose “el *Mossad*” desfiguró el sitio cibernético del presidente iraní, estableciendo firmemente

que Irán apoyaba a las organizaciones terroristas con sede en el Líbano.

La guerra cibernética se intensifica horizontalmente y más rápidamente que en la guerra común o estándar debido a tres razones. En primer lugar, el criterio principal para que existan ataques por parte de *hackers* civiles es la vulnerabilidad y no el estado crítico del blanco. La búsqueda de blancos vulnerables se amplía hasta que se encuentra uno. Si los sitios cibernéticos gubernamentales o comerciales en la nación que es el objetivo no son suficientemente vulnerables, los sitios que pertenecen a naciones amigas a la nación que se desea atacar cibernéticamente, a su vez se convierten en blancos. A la inversa, *hackers* profesionales empleados por una nación específica probablemente sólo intensificarán sus ataques si necesario para obtener las deseadas repercusiones en la nación que sirve de objetivo principal.

En segundo lugar, grupos internacionales de *hackers* ven a la situación como si fuese una sola en la cual pueden ejercer el poder sin temor al contraataque. Muchos *hackers* desean demostrar que apoyan una causa. Debido a

En segundo lugar, grupos internacionales de hackers ven a la situación como si fuese una sola en la cual pueden ejercer el poder sin temor al contraataque. Muchos hackers desean demostrar que apoyan una causa. Debido a que la red contiene métodos de difusión públicos incrustados, piratear cualquier blanco que pertenece a la red mundial tiende a ganar notoriedad.

que la red contiene métodos de difusión públicos incrustados, piratear cualquier blanco que pertenece a la red mundial tiende a ganar notoriedad.

En tercer lugar, conflictos cibernéticos hasta ahora han sido polarizados, o son bipolares. En cuanto más un conflicto sea bipolar, tal como el conflicto árabe-israelí, mayor es la posibilidad que atraerá voluntarios que desean trabajar por uno de los lados. Cada lado percibe al otro como teniendo aliados permanentes que siempre respaldarán sus enemigos. Por lo tanto, los EE.UU. fueron declarados un objetivo conjuntamente con Israel poco tiempo después del comienzo del conflicto cibernético palestino-israelí.²⁹

Tradicionalmente, los aliados de los países en guerra estaban en una situación bastante segura en cuanto a posibles ataques militares al menos que participaban directamente en el combate. El costo de provocar a una nación neutral al combate usualmente traía aparejado una penalidad a la nación que estaban escogiendo intensificar dicho conflicto. En el espacio cibernético, no obstante, el

costo de tal intensificación es pequeño para una nación, y casi inexistente para un *hacker* individual. Por ende, la rápida intensificación horizontal ocurrirá probablemente en futuros conflictos cibernéticos.

Fase 3: Rápida Internacionalización de Entidades No Estatales. El conflicto cibernético tiene la tendencia de atraer dos tipos de actores. El primer tipo incluye a grupos de *hackers* talentosos quienes se hallan involucrados a menudo en incidentes cibernéticos internacionales. El segundo tipo consiste en *hackers* aficionados atraídos por un fervor patriótico o ideológico. El conflicto cibernético palestino-israelí atrajo a *hackers* provenientes de Israel, Palestina, El Líbano, Alemania, Arabia Saudita, Paquistán, Brasil y los Estados Unidos. La mayoría de los ataques en contra de Israel fueron iniciados desde afuera de Israel o de la Autoridad Nacional Palestina.³⁰ Vale la pena resaltar es que uno o más grupos brasileños de *hackers* atacaron a ambos lados del conflicto palestino-israelí, aparentemente para demostrar quienes eran los participantes en cada lado. La escaramuza cibernética estadounidense-china atrajo a *hackers* simpatizantes de los EE.UU, Arabia Saudita, Paquistán, India, Brasil, Argentina y Malasia. Dentro del grupo de *hackers* simpatizantes del lado chino, se hallaban unos provenientes de la China, Japón, Indonesia y Corea. Se debe mencionar que las alineaciones de los *hackers* no necesariamente satisfacían los deseos de la nación, con excepción de aquellas naciones en donde el gobierno controla severamente el uso del Internet.

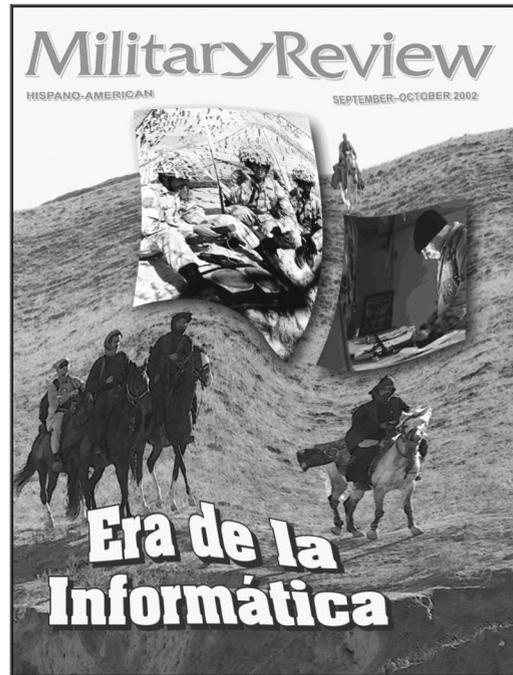
El grado de participación internacional que se observa en los conflictos cibernéticos tiene paralelos impresionantes con el grado de voluntarios durante la Guerra Civil española, una precursora de la II GM. El conflicto entre fascistas de un lado y comunistas y demócratas en otro, atrajo a gran número de voluntarios extranjeros a ambos lados. Tanto en la Guerra Civil española y el conflicto cibernético palestino-israelí, la ideología y no el lucro fue el que motivó a tales voluntarios. Existen *hackers* mercenarios, pero no se ha informado que están en un estado activo ya sea en el conflicto palestino-israelí como en el estadounidense-chino.

La mayoría de los *hackers* involucrados en los anteriormente mencionados conflictos eran veteranos de anteriores guerras cibernéticas internacionales. Los *hackers* paquistaníes, por ejemplo, habían estado también involucrados en desfigurar sitios cibernéticos en la India así como ciertos *hackers* brasileños habían estado involucrados en desfigurar sitios estadounidenses.³¹

“*Hactivism*” o la actividad de piratear lo sitios cibernéticos es tentadora cuando los *hackers* tienen el poder de participar en el escenario internacional.³²

Un *hacker* o un grupo pequeño de *hackers*, pueden causar tremendo daño en poco tiempo. Durante el conflicto estadounidense-chino, un grupo de *hackers*

denominado “PoizonB0x” afectó exitosamente a más de 400 sitios cibernéticos (*.cn) chinos.³³ Un informe estimaba que sólo habían unos 30 *hackers* principales involucrados en el conflicto cibernético palestino-israelí quienes proporcionaban los instrumentos, mientras que los involucrados sólo en las escrituras proporcionaban la “fuerza bruta” en cuanto a chequear y cerciorarse de las vulnerabilidades de los potenciales blancos.³⁴ La fuerza bruta de la serie 209 IP trata con el permiso de *hackers* chinos de descubrir la presencia de una red de transmisión de pruebas no segura del poder eléctrico en el estado de California.³⁵



Aún si el golpe inicial cibernético de un futuro conflicto es una acción militar bien coordinada, voluntarios provenientes de varias naciones probablemente estarán involucrados en ataques similares o mímicos, complicando así las operaciones de combate de la guerra real. Esta amenaza por sí sola tiene numerosas implicancias para la soberanía nacional y el derecho internacional.

Fase 4: Aprendizaje Global y el Aumento de Desarrollo y Proliferación de Armas Cibernéticas. Los instrumentos empleados y mejorados para ejecutar la piratería cibernética en el conflicto palestino-israelí aparecieron seguidamente en otras acciones internacionales y nacionales de piratería cibernética. Durante la guerra cibernética palestina-israelí, los *hackers* israelíes desarrollaron un nuevo instrumento para el método de ataque *DDoS*. *Hackers* adolescentes en los EE.UU. adquirieron dicho instrumento de los *hackers* israelíes y planearon un ataque global del Internet que se llevaría a cabo en el día de año nuevo del año 2001. De no ser que el *FBI* fue alertado del complot, el ataque hubiese podido ser exitoso en obstruir el uso del Internet ese día.³⁶

Durante la escaramuza estadounidense-china se inició el ataque *Carko DDoS*.³⁷ No sólo un agente del mencionado ataque intentó derrumbar el sistema que servía de blanco, empleó un ataque pulidor de sobrecarga para insertar una nueva contraseña de raíz, o instaló una nueva puerta trasera al sistema que servía de blanco mientras que el mismo se recuperaba del ataque. Esto significaba que aquellos sistemas que fueron derrumbados por los ataques *Carko* debían ser chequeados para ver si existía *software* que podría per-

mitir la penetración posterior del sistema.

A pesar que los ataques *DDoS* eran conocidos y empleados antes que este conflicto, la habilidad de una persona con un ancho de banda limitado de poder ejecutar un ataque *DDoS* a gran escala es un desarrollo reciente. Este tipo de ataque puede emplear un módem de 56 KB y una línea de subscripción digital asimétrica para comenzar el ataque, que posteriormente es incrementado 10.000 veces por difusores de servicios de la red para generar ataques de una magnitud de dos tercios de una línea *T1*. “Con instrumentos como estos, un módem de 56 KB puede convertirse en un arma poderosa y su ancho de

banda es irrelevante” resalta Ben Venzke, de *iDefense*.³⁸ Unos cuantos ataques coordinados provenientes de unos cuantos *laptops* a través de módems, por lo tanto, podrían generar a ataque combinado equivalente a varias líneas *T1* o aún una *T3*. Tal ataque podría abrumar la mayoría de los sistemas.

Además de los ataques *DDoS* iniciados a través de sitios de difusión, existe una técnica a través de la cual los *hackers* pueden colocar *software* en otros servidores del *Internet* y posteriormente activarla en un momento determinado. Estos servidores infectados son denominados *sombies* ya que participan sin saberlo o inconscientemente en ataques *DDoS*.³⁹

En general, el índice de desarrollo de armas cibernéticas tiende a incrementar durante los conflictos cibernéticos, tal como la invención de nuevas armas es más rápida y común durante la guerra. Lo que es aun más amenazador, sin embargo, es que el índice de proliferación de armas cibernéticas es más rápido que la proliferación de armas tradicionales.

Implicancias a la Política

Basado en estos acontecimientos existen cuatro necesidades en la política nacional e internacional:

- Decidir quién proporcionará seguridad en la Red.
- Proporcionar respuestas legales a la rápida intensificación horizontal.
- Poner en vigencia responsabilidades legales para ciudadanos *hackers* que son responsables de incidentes internacionales.
- Detener la proliferación de armas cibernéticas.

¿Quién proporcionará seguridad en la red? El cuestionamiento central referente a la política asociada al costo de conducir actos comerciales en la Red es, “¿Quién es el responsable de garantizar la seguridad en la Red?” ¿Son los responsables las grandes ISP, Corporaciones, el Gobierno, o permanecerá el Internet siendo una zona de fuego libre?⁴⁰

Algunos países han escogido asignar la seguridad de la Red al gobierno, especialmente en países en donde el Internet es considerado ser una amenaza al poder absoluto del gobierno, tal como lo es en la China. La mayoría de los países europeos están promulgando leyes que establecen al gobierno como el garante central de la seguridad de la Red.

A medida que las economías y las comunicaciones dependen más en el Internet, los países escogerán opciones que los colocan en algún lugar a lo largo del espectro de seguridad *versus* la privacidad. En la mayoría de los casos las leyes protegerán la seguridad en la Red

En tercer lugar, conflictos cibernéticos hasta ahora han sido polarizados, o son bipolares. En cuanto más un conflicto sea bipolar, tal como el conflicto árabe-israelí, mayor es la posibilidad que atraerá voluntarios que desean trabajar por uno de los lados. Cada lado percibe al otro como teniendo aliados permanentes que siempre respaldarán sus enemigos. Por lo tanto, los EE.UU. fueron declarados un objetivo conjuntamente con Israel poco tiempo después del comienzo del conflicto cibernético palestino-israelí.

por encima de la privacidad individual.⁴¹ Los Estados Unidos deberán decidir dónde en este espectro operará y qué nivel de seguridad cibernética deberá proporcionar para apoyar la seguridad de las transacciones y una cierta medida de privacidad.

Respuesta Legal a la Rápida Intensificación Horizontal. Cuan más elevada es la visibilidad del conflicto cibernético, cuánto más atraerá a los *hackers* internacionales, y cuán más rápidamente los mismos buscarán los sitios vulnerables. ¿Cuáles son las alternativas legales de un país atacado en un conflicto en el cual no está involucrado? Para obtener una respuesta legal, la identidad del perpetrador debe ser establecida. No obstante, los ataques cibernéticos no son iniciados con frecuencia por un país, sino más bien por un ciudadano. Es difícil de justificar un bombardeo de contraataque en contra de *hackers* que han violado la neutralidad u obediencia de sus propios países frente a otros. La piratería cibernética es una amenaza

asimétrica por parte de actores no estatales lo cual hace que un contraataque justificado sea difícil.

Se puede hacer poco en el espacio cibernético a los *hackers* debido a que no presentan un objetivo determinado. Los mismos tienden a no ser dueños de infraestructuras que pueden servir de blancos aún en el espacio cibernético. Cuando existe tal infraestructura, tener acceso a la misma legalmente es difícil debido a la soberanía nacional. Cuando los Estados Unidos, por ejemplo, llevó a cabo una operación policial en contra de dos *hackers* rusos, emergieron asuntos relacionados con el debido proceso debido a la búsqueda electrónica a larga distancia por parte del FBI de las computadoras de los *hackers* en Rusia.⁴² Cualquier respuesta debe considerar el posible daño colateral potencialmente causado por tal contraataque. Ya que *hackers* tienden a conducir sus ataques a través de varios servidores de terceros, cualquier contraataque cibernético debe tomar en consideración el hecho de que el contraataque puede afectar los servidores de víctimas inocentes.

En general, los países necesitan definir su autoridad legal para ejercer la soberanía, perseguir e imponer penalidades a *hackers* que han sido sentenciados de haber cometido ataques cibernéticos. Acuerdos internacionales que establecían no proteger a secuestradores aéreos contribuyeron significativamente a la disminución de tal crimen. Acuerdos internacionales similares referentes al crimen en el espacio cibernético ayudaría a disminuir los refugios disponibles a los *hackers*.

Responsabilidad Legal. Cada país debe encarar el hecho de que sus ciudadanos *hackers* pueden causar incidentes internacionales que son contrarios a sus intereses. Israel fue forzado en un conflicto cibernético por acciones de sus propios *hackers* adolescentes, y no debido a una decisión gubernamental. Israel no estaba preparado a entablar una guerra cibernética y era más vulnerable que su adversario.

Violaciones cibernéticas entre redes cibernéticamente interconectadas yacen en un área gris de las leyes de seguridad internacionales y nacionales. Para localizar y enjuiciar a los *hackers*, los países deben depender de las autoridades y de las leyes de la nación anfitriona del *hacker*. Israelí estimó que el daño causado por el virus global denominado “Love” (amor), incluyendo la interrupción de servicios de compañías telefónicas celulares alcanzó unos US\$12 millones. Sin embargo, Israel no pudo presentar cargos criminales en contra del *hacker* porque su país (las Filipinas) no estipulaba que escribir programas que podían causar un virus era un delito criminal hasta después de haber sido perpetrado.⁴³

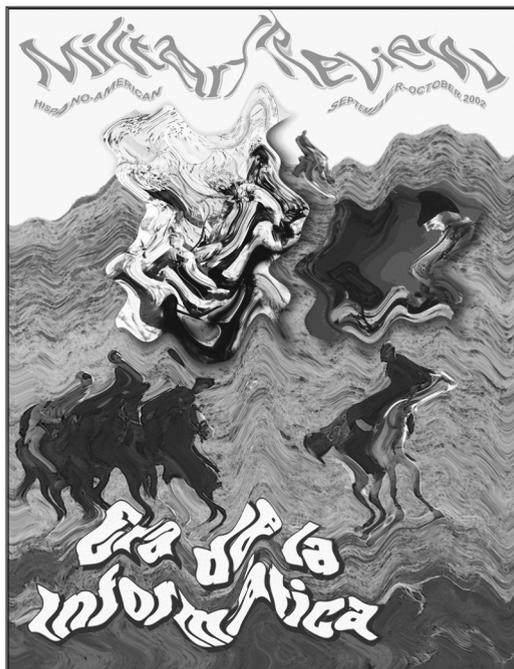
El castigo criminal es en particular difícil cuando los *hackers* operan desde un país obviamente hostil. No obstante, los países tienen ciertos derechos bajo el principio protector internacionalmente reconocido

en el caso de que las naciones que ofenden no ayuden. Existe un caso internacional de derecho, aunque limitado, que puede apoyar la acción del estado como respuesta a los ataques cibernéticos. Bajo este principio, cuando una persona de un país A hiere al país B, y el país A no previene que dicha persona continúe causando daño, entonces el país B puede entablar una acción judicial en contra del país A.⁴⁴ A pesar de que este principio no ha sido aún aplicado en casos relacionados con la guerra cibernética, el precedente legal existe.

Si un país tiene la intención de tratar a los *hackers* como criminales y terroristas, su política debe ser diseñada para exterminar cualesquiera actividades de piratería, aún las de menor importancia. Tal política de seguro alienaría a sus ciudadanos *hackers*. Juzgando sus propuestas leyes cibernéticas, la mayoría de las naciones europeas aparecen dirigiéndose hacia esta dirección.⁴⁵

Es improbable que los EE.UU. aplique una medida de fuerza sobre sus *hackers* nacionales. Tal medida no sólo sería innecesaria, sino contraproducente. Una opción que posiblemente tendrá éxito es el de proporcionar incentivos para los *hackers* de “sombrero blanco” (individuos que buscan identificar flaquezas en los sistemas de ciertas compañías y luego informar acerca de dichas flaquezas a las compañías cuyos sistemas penetraron). Estos *hackers* tienen interés en ayudar a otros y no causan daño. Se debería incentivar a dichos *hackers* a localizar las vulnerabilidades y ayudar a los administradores del sistema a aplicar los parches necesarios. Agentes de seguridad gubernamentales o privados podrían verificar que el parche es correcto y que no incluye una puerta de acceso trasera. Los *hackers* de sombrero blanco podrían ser públicamente recompensados y contratados como asesores independientes referente a otras soluciones al estilo sombrero blanco. La labor de dichos *hackers* debería ser confirmada, sin embargo no deberían ser necesariamente controlados o empleados oficialmente por el gobierno. La imagen de independencia, además de hacer lo que es correcto, posee un gran atractivo entre los *hackers* de sombrero blanco.

Recíprocamente, los mencionados *hackers* deben ser identificados y enjuiciados. El sistema legal debe desarrollar una completa gama de sanciones formales en contra



de la piratería cibernética y sus diversas actividades. Actualmente, agencias estatales y federales en los EE.UU. están deplorablemente no calificadas para lidiar el grado y nivel de acciones de piratería cibernética.⁴⁶ Una dificultad de mayor importancia es que es difícil para el gobierno atraer y retener especialistas computacionales habilidosos debido al bajo sueldo que puede ofrecer.⁴⁷

Una alternativa tal vez sea el uso de *hackers* de sombrero blanco para hallar los de sombrero negro en el espacio cibernético. Las fuerzas militares dedicadas a desviar, averiar, rastrear y castigar a los piratas cibernéticos más importantes en contra de intereses de los EE.UU. y del mundo tal vez

puedan mantener el orden en la Red mundial y evitar la intensificación de los conflictos cibernéticos.⁴⁸

La Respuesta Internacional

Cada escaramuza cibernética impulsa el desarrollo de nuevas armas cibernéticas, las cuales subsecuentemente diseminadas rápidamente a los *hackers* profesionales y aficionados alrededor del mundo. La proliferación tiene implicancias significativas en el monitoreo de las herramientas de *hacking* empleadas en los conflictos y en las nuevas tecnologías del Internet en general. Además de monitorear las capacidades de estas nuevas herramientas, las naciones del mundo deben monitorear los *chat-rooms* en los cuales los *hackers* aficionados no pueden resistir la tentación de jugar con el nuevo juguete. Los *hackers* patrocinados por un estado no emplearán la arma nueva a menos que sea parte de un plan general, para que no pierdan el elemento de sorpresa. Por lo tanto, cada país debe desarrollar contramedidas para ayudar a prevenir el empleo de nuevas armas cibernéticas o suavizar sus efectos. Debemos hacer revisiones rutinarias en los servidores para el *software* *sombie* que permite los ataques *DDoS* sean lanzados para minimizar la magnitud de futuros ataques. Al mantenerse con el ritmo de nuevas herramientas y métodos de *hacking*, una nación puede estar mejor preparada para evitar o minimizar sus efectos.

En cualquier conflicto moderno, el espacio cibernético puede ser otra ruta de ataque. En cuanto que los EE.UU. es el más grande actor en el ambiente político internacional, ha llegado a ser un pararrayos para los *hackers*

y ataques terroristas, no obstante si la nación estuviese involucrada en el conflicto inicial. Hasta el 11 de septiembre de 2001, los EE.UU. era, en general, complaciente con respecto a sus enemigos en ultramar. Sin embargo,

la distancia entre los EE.UU. y sus enemigos ha sido dramáticamente reducida. Las lecciones de los primeros conflictos cibernéticos deben ser aprendidas ahora para estar mejor preparados para los futuros conflictos. **MR**

NOTAS

1. Peggy Weigle, Jefe oficial ejecutivo (CEO), Sanctum Inc., citada en Carmen J. Gentile, "Hacker War Rages In Holy Land", disponible en el internet en www.wired.com/news/politics/0,1283,40030,00.html, 8 de noviembre de 2000.
2. James Adam, CEO, iDefense, citado en Gentile, "Israeli Hackers Vow to Defend", en el internet www.wired.com/news/politics/0,1283,40187,00.html, 15 de noviembre de 2000.
3. "Cyber War also Rages in MidEast", *The Associated Press*, en internet en www.wired.com/news/print/0,1294,39766,00.html, 26 de octubre de 2000; Brian Krebs, "Hackers Worldwide Fan Flames in Middle East Conflict", en internet en www.infowar.com/hacker/00/hack_112000c_j.shtml, 20 de noviembre de 2000.
4. "Cyber War Also Rages in MidEast."
5. Krebs, "Hackers Worldwide"; Infowar.com, 20 de noviembre de 2000; "Israel's 'Mossad' Hackers Break into Iranian President's Website", *Xinhua News Agency Bulletin* (18 de enero de 2001); en internet en www.infowar.com/hacker/01/hack_011901c_j.shtml, 19 de enero de 2001; Tania Hershman, "Israeli Seminar on Cyberwar", en internet en www.wired.com/news/politics/0,1283,41048,00.html, 10 enero de 2001.
6. Gentile, "Palestinian Crackers Share Bugs", en internet en www.wired.com/news/politics/0,1283,40449,00.html, 2 de diciembre de 2000.
7. Robyn Welsman, "California Power Grid Hack Underscores Threat to U.S.", en internet en www.newsfactor.com/peril/story/11220.html, 13 de junio de 2001.
8. "Israel Suffers Escalating Hack Attacks", en internet en www.mi2g.com/cgi/mi2g/press/150402.php, 15 April 2002.
9. Gentile, "Israeli Hackers."
10. *Ibid.*, "Palestinian Crackers."
11. *Ibid.*, "Hacker War Wages."
12. *Ibid.*, "Israeli Hackers."
13. Krebs; Elisa Batista, "Palestinian Group Targets AT&T", en internet en www.wired.com/news/business/0,1367,39913,00.html, 6 de noviembre de 2000.
14. Gentile, "Israeli Hackers."
15. *Ibid.*, "Hacker War Wages."
16. *Ibid.*, "Israeli Hackers."
17. Michelle Delio, "It's (Cyber) War: China vs. U.S.", en internet en www.wirednews.com/news/print/0,1294,43437,00.html, 30 de abril de 2001.
18. *Ibid.*
19. Aviso Nro. 01-009 del Centro de Protección de Infraestructura Nacional de los EE.UU., "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May", en internet en www.nipcc.gov/warnings/advisories/2001/01-009.htm, 26 de abril de 2001.
20. Delio, "U.S., Chinese Hackers Wage Online War", *Agence France Presse* (24 de abril de 2001), en internet en www.inq7.net/inf/2001/apr/24/inf_3-1.htm, 24 de abril de 2001.
21. Gentile, "Palestinian Crackers" y "Israeli Hackers."
22. Elazar Levin, "Overseas Hackers Strike Again: Israel Land Administration Shuts Down Most of its Web Site", *Israel's Business Arena* (4 de diciembre de 2000), en internet en <http://new.globes.co.il/serveEN/globes/docView.asp?did=454769&fid=947>, y www.infowar.com/hacker/00/hack_120500a_j.shtml, 5 de diciembre de 2000.
23. Gentile, "Palestinian Crackers".
24. Lawrence K. Gershwin, "Cyber Threat Trends and US Network Security", en una declaración ante el Comité Económico Conjunto, en internet en www.cia.gov/cia/public_affairs/speeches/gerhswin_speech_062, 21 de junio de 2001.
25. Matt Krantz y Edward Iwata, "Companies Bleed Cash When Computers Quit", *USA Today*, 11 de junio de 2001, sección B, pág. 1.
26. "Israel Suffers."
27. Delio, "Got a Virus? Blame the Tightwads", en internet en www.wired.com/news/technology/0,1282,42047,00.html, 28 de febrero de 2001.
28. "Cyber War Also Rages"; Krebs, "Hackers Worldwide."
29. Gentile, "Hacker War Rages."
30. *Ibid.*, "Israeli Hackers."
31. Robert MacMillan, "Hackers Deface Policy.com as 'Public Service'", *Newsbytes*, Washington, D.C., en internet en www.infowar.com/hacker/00/hack_111500a_j.shtml, 15 de noviembre de 2000.
32. Carrie Kirby, "Hacking with a Conscience is a New Trend", *San Francisco Chronicle*, 20 de noviembre de 2000, en internet en www.infowar.com/hacker/00/hack_112400a_j.shtml, 24 de noviembre de 2000.
33. John Lyman, "Hackers Aim at Computer Security Sites", en internet en www.newsfactor.com/peril/printer/11230, 14 de junio de 2001.
34. Gentile, "Palestinian Crackers."
35. Welsman, "California Power Grid."
36. Krebs, "FBI Arrests Hacker in Planned New Year's Eve Attack", *Newsbytes*, Washington, D.C. (12 de enero de 2001), en internet en www.infowar.com/hacker/01/hack_0111501b_j.shtml, 15 de enero de 2001; y "Feds Warn of Concerted Hacker Attacks on New Year's Eve", *Newsbytes*, Washington, D.C., en internet en www.infowar.com/hacker/00/hack_122900a_j.shtml, 29 de diciembre de 2000.
37. Steve Gold, "More Details Emerge on Expected Chinese Hack Attacks", *Newsbytes*, Parsippany, Nueva Jersey (27 de abril de 2001), en internet en www.infowar.com, 27 de abril de 2001.
38. Gentile, "Palestinian Crackers."
39. Krebs, "Feds Warn...".
40. Chris C. Demchak, "State Security Paths in a Digital Mass Society: New Internet Topologies and Security Institution Obligations", *Cambridge Review of International Affairs*, número especial sobre la seguridad del estado y el internet, fecha desconocida.
41. Bob Sullivan, "Cybercrime Treaty Targets Hackers", *MSNBC News*, en internet en www.msnbc.com:80/news/480734.asp, 6 de noviembre de 2000, y www.infowar.com/hacker/00/hack_110600e_j.shtml, 6 de noviembre de 2000.
42. Thomas C. Greene, "FBI Hacked Russian Hackers", en internet en www.theregister.co.uk/content/8/18496.html, 25 de abril de 2001.
43. Israeli Consulate Online Service (IsraelLine), "Love Virus Hits Israeli Businesses", Nueva York, 8 de mayo de 2000; Lynn Burke, "Love Bug Case Dead in Manila", *Wired Online*, 21 de agosto de August 2001.
44. Iain Cameron, Protective Principle of International Criminal Jurisdiction (Dartmouth, Massachusetts: Dartmouth Publishing Company, 1993).
45. Sullivan, "Cybercrime Treaty."
46. Greg Farrell, "Police Outgunned by Cybercriminals", *USA Today*, 6 de diciembre de 2000, en internet en www.infowar.com, 7 de diciembre de 2000.
47. Patrick Thibodeau, "CIO Panel Recommends Hiring IT Rookies", *Computerworld*, en internet en <http://iwsun4.infoworld.com/articles/hn/sml/00/10/12/001012hhiring.xml>, 12 de octubre de 2000.
48. Demchak, "State Security Paths."

El coronel Patrick D. Allen, Componente de Reserva del Ejército de los EE.UU., es ingeniero con mayor jerarquía de sistemas, para el Sistema de Información Avanzada de General Dynamics, Operaciones de Información en Arlington, Virginia. Él obtuvo una licenciatura en Física y una maestría en Ingeniería Industrial e Investigación de Operaciones, una segunda maestría en Estudios Estratégicos y un doctorado en Economía Mineral e Investigación de Operaciones y además es egresado de la Escuela de Comando y Estado Mayor del Ejército, la Escuela Superior de Guerra del Ejército y la Escuela Superior de Guerra Aérea. Se han publicado más de 40 de sus artículos referentes a los temas de programación y simulación y operaciones de información.

El teniente coronel Chris C. Demchak, Componente de Reserva del Ejército de los EE.UU., es co-fundador del Grupo de Investigación de la Política del Espacio Cibernético, un grupo transnacional de expertos que documentan y estudian la expansión global de las tecnologías de la Red y sus efectos en agencias nacionales militares y otras. Ella obtuvo una maestría en Desarrollo Económico y otra maestría en Ingeniería de Energía y además obtuvo un doctorado en Ciencias Políticas con un enfoque en la Teoría de Organización y Sistemas Complejos. Ella ha llevado a cabo y ha dirigido estudios empíricos y profundos acerca de los Ejércitos de los EE.UU. de Gran Bretaña e Israel y análisis de las implicancias de modernización democráticas civil-militar en las FF.AA. de Europa Central. Muchos de sus artículos han sido publicados así como su libro titulado "Military Organizations, Complex Machines: Modernization in the U.S. Armed Services".