r.esici.10(19):57-69,2018

Estrategias de ciberguerra: Israel y Rusia[1]

Javier Alejandro Guayara Arciniegas[2, *]

Resumen

La guerra no es un fenómeno estático, cambia, evoluciona, se adapta a las nuevas realidades; vivimos en un mundo con enorme dependencia de las tecnologías de la información y la telecomunicación, nuevos actores surgen y amenazan la seguridad de los Estados haciendo uso de las mismas herramientas que empleamos a diario, los hackers se han convertido en algo que preocupa a los gobiernos del mundo, poseen un nivel de conocimientos que puede poner en peligro infraestructuras críticas de los países, pero ¿qué pasa cuando ya no sólo se debe preocupar por las acciones perpetradas en el ciberespacio por individuos aislados? sino que además, debe preocuparse por otros Estados con grandes fuentes de recursos económicos, que deciden profesionalizarse para hacer uso bélico de las herramientas electrónicas y de programación; este es el mundo en el que estamos inmersos hoy, el nuevo escenario de la guerra y quienes mejor ejemplifican esta realidad son Rusia e Israel.

Palabras clave: ciberguerra, hacker, ciberespacio, código malicioso.

Clasificación JEL: K22, K33, F13, F42

[1] Artículo de investigación.

[2] Tecnólogo en Ciencias Militares, Escuela de Suboficiales Inocencio Chinca.

[*] javierguayara2012@gmail.com.

Fecha de recepción:
10 de febrero de 2018.

Fecha de aceptación:
23 de junio de 2018.

Para citar este artículo:
Guayara, J. (2018). Estrategias de ciberguerra: Israel y Rusia. *Perspectivas en inteligencia*, *10*(19): 57-69.

Abstract

War is not a static phenomenon, it is changing, evolving and adapting according to the new reality, we are living in a dependent world on information and telecommunications technology, where new actors are emerging to threat the states security through same tools that we use every day, hackers have become a concern to governments around the world, they have a knowledge level able to endangers the infrastructure of the countries, but What is happening when they not only have to worry about perpetrated actions by isolated individuals in cyberspace? But it should be worried about other states with many sources of economic resources, which decide become professionals to war using both electronic and programming tools, this is the world in which we are engaged today, the new war stage where Russia and Israel are the best example

Keywords: cyberwar, hacker, cyberspace, malicious code.

JEL classification: K22, K33, F13, F42.

Introducción

Históricamente, una de las formas más comunes de interacción entre los pueblos ha sido la confrontación bélica. Se tiene registro de enfrentamientos violentos entre grupos humanos casi desde el comienzo mismo de la civilización, pero la guerra no es un fenómeno que se haya repetido de manera idéntica a lo largo de la historia, pues con el paso del tiempo evolucionó y continúa haciéndolo. Son múltiples los estudios que han dedicado su atención a caracterizar la evolución de las formas y medios de hacer la guerra y algo que siempre ha jugado un papel determinante en la manera de ejercer la violencia es el nivel de desarrollo tecnológico disponible en el momento, además de tener la capacidad táctica y técnica para hacer buen uso de la misma.

Esta época no sería la excepción: los avances tecnológicos han cambiado por completo las concepciones clásicas de la guerra, cada vez se desdibujan más las fronteras nacionales y el accionar de los ejércitos responde a estrategias nuevas, vinculadas estrechamente con las nuevas y avanzadas tecnologías de la información. Es así como hoy hablamos de un nuevo escenario del conflicto: el ciberespacio.

La seguridad cibernética cada vez representa un papel más importante en la agenda de los estados, que se han percatado del gran potencial que existe en este entorno para ser usado como la plataforma de un gran ataque. La situación va más allá de lo que un observador poco conocedor del tema puede pensar: los ataques que pueden ser perpetrados a través del ciberespacio tienen la capacidad de llegar a ser tan devastadores como los realizados con misiles (Russia Today, 2012).

Los expertos hablan de una ciberguerra, un fenómeno en el que podríamos estar inmersos ahora mismo sin siquiera haberlo percibido; la definición de esta palabra no reviste mayor complejidad de la aparente, simplemente se trata de un choque "violento" entre grupos organizados de personas que tienen lugar en el ciberespacio. El término viene acompañado normalmente de otras expresiones igualmente transparentes como ciberataque, cibercomando, ciberdefensa, ciberespionaje, cibersabotaje, entre otros.

Este nuevo paradigma ha hecho que muchos estados se interesen por fortalecer su posición en el nuevo escenario de la guerra. La carrera fue inicialmente emprendida por los estados más desarrollados y aquellos que tenían un mayor grado de especialización en el uso de tecnologías de información, por ejemplo, Estados Unidos, China, Rusia, Reino Unido, Israel, Alemania y Francia. La

creación de cibercomandos ha sido la manera habitual de responder a estas nuevas amenazas, pues estos hacen referencia a divisiones completas de los ejércitos dedicadas a la protección y respuesta a ciberataques y su accionar es casi idéntico al llevado a cabo por unidades militares en el campo de batalla, tal y como lo explica Jorge Soriano (s.f). Estos estarían compuestos por tres escuadrones: uno de *reconocimiento*, que buscaría obtener la mayor cantidad de informacion del adversario, como el tipo de tecnología usada y puntos débiles; luego un escuadrón de *asalto* que, bajo las órdenes de un general, realizaría actividades destinadas al rompimiento de las defensas, ocultando su presencia para finalmente modificar, robar o destruir informacion u operaciones del sistema, siendo apoyados por un tercero, sin mayor participacion en el campo de batalla, pero que es fundamental para el accionar de los dos primeros, que es el escuadrón de *inteligencia*, dado que su objetivo es estudiar las vulnerabilidades de cualquier hardware o software blanco del ataque, para finalmente producir herramientas que sean útiles para explotar estas debilidades.

Este artículo tiene por objeto de estudio, principalmente, los casos ruso e israelí, naciones que han ganado fama por ser los presuntos perpetradores de grandes ataques a otros estados usando diferentes estrategias de ciberguerra.

Israel

El Estado hebreo ha gozado de un apadrinamiento americano desde el momento mismo de su nacimiento en 1948 y, gracias a múltiples acuerdos de cooperación, ha logrado alcanzar un grado de desarrollo tecnológico y militar que le ha permitido sobrevivir en una región totalmente hostil a la presencia judía. Es de conocimiento general el grado de sensibilidad que tiene esta región y cómo los estados allí situados están permanentemente listos para la guerra, en especial Israel que no tiene ningún vecino amistoso. Este escenario le ha llevado a centrar todos sus esfuerzos en defensa aún en tiempos de "paz"; todos los escenarios del conflicto han sido cubiertos por el Estado judío, incluyendo el ciberespacio, campo en el que se destaca por estar a la vanguardia.

El Grupo Nacional de Tareas Cibernéticas es la entidad israelí encargada de la seguridad en el ciberespacio de ese país. La creación de este organismo fue anunciada a comienzos del 2011 por el primer ministro israelí Benjamin Netanyahu, está conformado por 80 personas al mando de un general jubilado, cuenta con un presupuesto de cientos de millones de shekels y tendría fines estrictamente defensivos (Reuters, 2011), aunque se sabe bien que hace mucho Israel viene adelantando tareas especiales con fines bélicos en el ciberespacio,

con acciones que dan cuenta de las avanzadas herramientas tecnológicas desarrolladas la cuales, lejos de ser diseñadas para la defensa, poseen cualidades que las configuran como avanzadas ciberarmas, tal es el caso del mundialmente famoso gusano Stuxnet y la ciberarma Flame.

Para nadie es un secreto que la más grave amenaza percibida por el gobierno israelí, actualmente, es el programa nuclear iraní. Mucho se especuló sobre la posibilidad de un bombardeo por parte de Israel a las plantas de enriquecimiento de uranio de la república islámica. La reacción de Israel ante tal desafío, más allá de estas conjeturas, fue el sabotaje de las instalaciones mediante la utilización de un sofisticado código malicioso llamado Stuxnet, aunque cabe aclarar que la autoría del ataque jamás fue confirmada por las autoridades israelíes, pero todo apunta en esa dirección.

Las características del código malicioso son especialmente avanzadas: cuando fue descubierto, el virus fue catalogado como la más compleja y poderosa pieza de malware jamás vista, según estudios realizados por un equipo de consultores alemanes liderados por Ralph Langner (2011) que revelaron varios aspectos interesantes sobre la naturaleza del gusano, que apuntan a que "Stuxnet" es una sofisticada ciberarma que tenía claramente identificado su objetivo, tanto que el equipo decidió experimentar con el complejo software e infectar su propio entorno para estudiar su comportamiento y lo que sucedió fue bastante curioso: en palabras del propio Langner, "el gusano se comportaba como una rata de laboratorio a la que no le gustaba el queso que se le estaba ofreciendo, lo olía pero no lo quería comer" (2011). Este no suele ser un comportamiento habitual de un virus computacional, lo que les llevó a experimentar con diferentes "sabores de queso"; el estudio realizado por estos hombres fue arduo, tuvieron que contemplar una gran gama de posibilidades, hacer conjeturas acerca de cuál podría ser su objetivo en el mundo real y relacionarlas con alrededor de 15.000 líneas de las que estaba compuesto el código, infiriendo que este seguramente estaba en Irán, donde se encontraban la mayor cantidad de computadores infectados. Luego de un análisis exhaustivo del código, se toparon con un número que era bastante repetitivo "164", por lo que se dedicaron a estudiar cuál podría ser la relación que tenía este número con alguno de los posibles blancos estratégicos situados en Irán y encontraron una asombrosa coincidencia: la planta de enriquecimiento de uranio de Natanz estaba construida utilizando algo que en lenguaje técnico se conoce como sistema de cascada, y cada una de ellas contiene 164 centrífugas.

Todo indicaba que el objetivo era esta planta iraní dado que, luego de experimentar con este nuevo "queso", se dieron cuenta de la increíble capacidad de Stuxnet, puesto

que muchos de los sistemas de esta planta son controlados por computadoras considerando que existen operaciones que requieren ser efectuadas en cuestión de milisegundos, imposibles de ser realizadas por operadores humanos. Allí el intrincado malware atacaba, siendo capaz de modificar los datos de entrada de estas computadoras y haciendo que la respuesta emitida no fuera la esperada. Su complejidad es tal que, en un caso hipotético, hubiera podido arruinar por completo las instalaciones o incluso hacerlas explotar sin siquiera haber sido percibido por alguno de los miembros del personal.

Las características del gusano Stuxnet son tan avanzadas que las investigaciones descartan por completo la posibilidad que hubiera sido diseñado sin apoyo gubernamental. No sólo eso: debido a la naturaleza del objetivo, a la manera cómo fue realizada la operación, a las rivalidades políticas y al grado de sofisticación de la ciberarma, es ampliamente aceptada la hipótesis que Israel es el directo responsable del ciberataque. A pesar de esto, Langner también considera que, aunque la ofensiva pudo haber sido efectuado por el Mosad, se requirió la ayuda de quien él considera "la única superpotencia cibernética" para la elaboración del complejo gusano: Estados Unidos.

Esta potente ciberarma fue hasta hace muy poco tiempo el más poderoso virus conocido, que palidecería ante el hallazgo, en 2012, de una herramienta aún más compleja: Worm.Win32. Flame o como es normalmente nombrado "Flame".

¿Qué se sabe de este código malicioso hasta el momento? Casi todo: el virus tiene un tamaño de 20 megabytes, gigantesco si se tiene en cuenta el tipo de software del que se está hablando, es 20 veces más grande que Stuxnet y sus capacidades son aún más impresionantes. Se trata de un software de espionaje, capaz de generar capturas de pantalla que permitirían ver lo mismo que ve el operador de la máquina infectada; captar conversaciones de internet; recoger conversaciones bluetooth; robar los datos guardados en el ordenador e incluso activar los micrófonos de los computadores para grabar los sonidos del entorno en el que se encuentra la máquina. Jamás se había visto tan elaborada pieza de software dedicada al espionaje y curiosamente, una vez más, la mayoría de computadoras infectadas se encuentran situadas en Irán (Reuters, 2012).

Kaspersky, famosa firma rusa fabricante de antivirus distribuidos a nivel mundial, fue quien descubrió el malware. Sus estudios son los que han determinado todas estas características hoy conocidas por la población y han trabajado arduamente para determinar cómo contrarrestarlo. La empresa afirma que se requiere ayuda gubernamental para crear un programa como este, pero se niega a señalar algún posible responsable.

El diario *Washington Post*, citando funcionarios occidentales anónimos, ha dicho: "El software malicioso (malware) bautizado Flame, tenía como objetivo diagramar un mapa de la red informática de Irán y espiar las computadoras de funcionarios iraníes" (Hosenball, 2012).

Pero quizás lo más revelador de la situación, es la evidencia técnica que vincula a Flame con el anteriormente nombrado Stuxnet. Especialistas en seguridad cibernética de Kaspersky aseguran que ambos programas poseen fragmentos de códigos idénticos y que utilizan las mismas técnicas de *exploit*, lo que los lleva a concluir que ambos programas fueron fabricados por la misma entidad, al explicar que "el código fuente es su más preciada posesión, su santo grial. Usted no sólo se lo regala a cualquiera" (Greenberg, 2012).

Las evidencias hacen que de nuevo la mirada se dirija a Estados Unidos e Israel como los autores de la ciberarma mencionada; los expertos de Kaspersky aseguraron también que el virus pudo haber estado trabajando en la sombra dos años antes (Euronews, 2012), que plantea la posibilidad que Stuxnet y Flame hayan trabajado de manera conjunta, lo cual concordaría perfectamente con la anteriormente citada teoría de Jorge Soriano acerca de la manera de actuar de los cibercomandos: primero, un escuadrón de reconocimiento, para el caso sería la puesta en marcha de Flame, utilizándolo para recoger toda la información necesaria, luego los datos recolectados serían usados por un escuadrón de asalto para realizar tareas de sabotaje, en las cuales el gusano Stuxnet habría sido el protagonista, cada uno de ellos apoyados por un escuadrón de inteligencia que aún hoy permanece en las sombras, pero que sin duda alguna fueron los responsables de la fabricación de tan sofisticadas armas. El accionar de Israel en la materia es vanguardista y actualmente no se tiene ningún reporte de un ataque similar en el algún lugar del mundo.

Aunque la autoría de los ataques jamás ha sido reconocida por el régimen sionista tampoco ha sido negada. Lejos de esto, las declaraciones del viceprimer ministro Moshe Yaalon fueron bastante comprometedoras, cuando se le preguntó acerca de Flame: "Quienquiera que vea a la amenaza iraní como una amenaza significativa probablemente tome varias medidas, incluso éstas, para obstaculizarla" o "Israel ha sido bendecido con alta tecnología y nos enorgullecemos de herramientas que nos abren todo tipo de oportunidades" (Reuters, 2012).

Con frecuencia se publican nuevas noticias que dan fe del temor que tiene Irán a los ataques israelíes en el ciberespacio. El jueves 21 de junio de 2012 el gobierno iraní denunció un nuevo plan de ciberataque que, según ellos, sería ejecutado

por Estados Unidos, Israel y el Reino Unido, en represalia por las infructuosas negociaciones adelantadas con el fin que la república islámica abandonara su programa nuclear. Las autoridades iraníes dijeron haber tomado las medidas de precaución necesarias para frenar el posible ataque y que *Flame* ya había sido controlado. Las declaraciones por parte del gobierno no dejaron muy claro si la nueva agresión que se esperaba hacía uso de la tecnología ya conocida o si se trataba de una nueva ciberarma (Reuters, 2012)

Rusia

El caso ruso es significativamente diferente al israelí. Cuando se analizan los hábitos y ventajas que tienen los hackers se hace evidente que estas varían de acuerdo al país del que provengan: es así como los chinos son reconocidos por el espionaje industrial, los brasileños por el fraude financiero y los rusos por la creación de herramientas sencillas de crackeo especiales para principiantes, esto según Alex Shipp empleado de la empresa MessageLabs especialista en seguridad informática (Arun, 2012). Y es precisamente esta ventaja la que se destaca cuando se habla de los ciberataques efectuados por los rusos a otros estados y, para explicarlo, abordaremos cada uno de los casos que más resonancia han tenido en los últimos años con relación al tema.

El primero y quizás más famoso de todos, fue el ataque sufrido por Estonia en el año 2007, que se configuró como un hito en materia de ciberseguridad, ya que encendió las alarmas de los demás estados al percatarse del peligro real representado por un ataque a través del ciberespacio. El 15 de abril de ese año, el gobierno de Estonia decidió remover un monumento que se encontraba en el centro de Tallin "El soldado de bronce", que había sido erigido en honor a los soldados caídos en las batallas libradas por la Unión Soviética contra la Alemania nazi en la Segunda Guerra Mundial.

Este acto del gobierno estonio provocó malestar en Rusia, conllevando a un fuerte enfrentamiento diplomático entre los dos países. El día 26 del mismo mes, se dio inicio a un gran ciberataque, usando la modalidad del clásico DDoS –técnica que será explicada más adelante–, que para el fin de esa semana ya se había provocado la caída de las principales páginas web gubernamentales y de los partidos políticos; durante la segunda semana se desconectaron todos los medios de comunicación, dejando a la nación sin posibilidad de alertar al mundo lo que estaba ocurriendo al interior del país; el 9 de mayo se desconectó el sistema financiero del país, todas las páginas de los bancos colapsaron y los cajeros automáticos dejaron de funcionar; finalmente, durante tres semanas

los sitios del gobierno, de los bancos y de las universidades fueron atacados y desconectados. El más grande ciberataque del que se tiene registro culminó el 19 de mayo del año 2007. Estonia culpó a Rusia por estas ofensivas, pero esto es algo que no ha podido ser demostrado (Ministerio de Defensa Nacional, 2009).

El gobierno estonio buscó una reacción mancomunada en el marco de la OTAN y de la UE, con el inconveniente que, para la fecha, no había protocolos que establecieran la postura que debían tomar tales organismos ante un ataque perpetrado a través de internet. Este no fue el único problema para reaccionar, la razón que más peso tenía y que evitó una respuesta en el marco de la OTAN era la falta de evidencia determinante para vincular directamente al Kremlin con los ataques ejecutados, dado que se hizo un rastreo de los ordenadores que realizaron el ataque localizándolos en Rusia, pero no hubo manera de demostrar que el gobierno fue quien dio la orden de consumarlos.

El *modus operandi* fue muy elemental: para realizar un DDoS no se requiere de la más avanzada tecnología y se sabe bien que para llevar a cabo estos ataques se infectan miles de computadoras, todos estos ordenadores de origen ruso pudieron haber estado bajo el control de algún software especializado usado para esta tarea, por lo que pudieron haber participado del ataque sin siquiera haberse percatado de ello.

La única acción que pudo ser realizada luego del ataque, aunque no menos importante, fue de carácter preventivo. En agosto de 2008, la OTAN creó el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD) en donde, al mando de una de sus divisiones, se encontraba el teniente coronel del ejército español Néstor Ganuza Artiles, quien ha hablado de algunas de las operaciones que son adelantadas por este organismo como "estudios sobre inteligencia artificial aplicada a ciberdefensa o la monitorización de la Red, con especial atención a la correlación de eventos de seguridad. También hacemos trabajos en el campo de la doctrina, formación, instrucción y entrenamiento. Además, desarrollamos conceptos de ciberguerra" (Criado, 2010).

Un caso más reciente fueron los ciberataques realizados a Georgia, en correspondencia con el conflicto bélico que se estaba viviendo en la región del Cáucaso, que tuvo su inicio en el año 2008 con un altercado militar entre Georgia en un bando y Osetia del sur, Abjasia y Rusia en el otro (Anónimo, 2010). Para este artículo no es relevante cuál fue la raíz histórica del conflicto ni cómo se desenvolvió en el campo de batalla físico, sólo resulta útil analizar la batalla que se libró en el ciberespacio por parte de hackers rusos.

De nuevo, la táctica utilizada fue el DDoS, que ocasionó que múltiples sitios web del gobierno georgiano fueron derribados, entre ellos la página oficial del presidente; particularmente, cuando se trataba de ingresar a la misma, se desplazaba hacia una nueva que contenía imágenes de dictadores del siglo XX junto a una del mandatario georgiano Mikheil Saakashvili; la mayoría de las páginas atacadas fueron simplemente bloqueadas y re-direccionadas a unas nuevas con propaganda pro rusa y algunas de ellas contenían mensajes tales como "win+love+in+Russia" (Markoff, 2008)

Los ciberataques no tuvieron mayor impacto a causa de la naturaleza misma de la agresión, pero también debido al bajo grado de penetración que tiene el internet en Georgia. De nuevo, el gobierno ruso declaró no estar implicado en las acciones y representantes de Rusia en Washington aseguraron ser incapaces de negar la posibilidad que personas de su país hayan decidido por propia voluntad inutilizar las páginas georgianas: "también hay este tipo de personas en Estados Unidos" (Markoff, 2008).

En ninguno de los dos casos mencionados se posee evidencia suficiente como para vincular al Kremlin directamente con los ataques, a pesar que tanto Estonia como Georgia lo señalan como el único responsable. El gobierno ruso de ningún modo ha anunciado formalmente la creación de un cibercomando y fue hasta hace muy poco que un documento oficial reveló el interés de Rusia en la ciberguerra. El documento se titula *Criterios conceptuales sobre la actividad de Fuerzas Armadas de la Federación de Rusia en el espacio informático*, fue escrito en el 2011 y publicado en la página del Ministerio de Defensa ruso al año siguiente. Su contenido no menciona cómo se gestionan las actividades ofensivas en el ciberespacio, simplemente se limita a plantear ciertos criterios de defensa, contención de ataques y cómo responder ante estos. Se cree que el documento pudo haber sido concebido en el marco del Servicio Federal de Seguridad (FSB) o por el Consejo de Seguridad adjunto a la presidencia (Meshcheriakov, 2012).

Las acciones llevadas a cabo en ambos casos son bastante simples, dado que los ataques del tipo DDoS son tan elementales que son también usados por organizaciones con mucho menos recursos, como por ejemplo Anonymous. La simpleza misma del ataque conlleva a que pueda ser aceptada la hipótesis acerca de la naturaleza no gubernamental del mismo, pero resulta bastante sospechoso que un idéntico tipo de ataque haya sido ejecutado en medio de las elecciones celebradas en el año 2011, definiendo como blanco los sitios web de medios de comunicación opositores y de ONGs que trataban de informar acerca de las irregularidades presentadas en el proceso político, los cuales fueron bombardeados con más de 50.000 solicitudes por segundo que eclipsaron por

completo sus servicios (Euronews, 2011). Sin embargo, nuevamente señalar a los responsables sólo se basa en conjeturas, por más obvio que parezca, pues no hay una forma legítima de comprobar la autoría de este tipo de ataques.

Análisis comparado

Como ya fue resaltado anteriormente, la forma en cómo se realizan los ataques en el ciberespacio es radicalmente diferente en cada uno de los casos estudiados. Curiosamente, el grado de profesionalización y sofisticación que estos poseen es significativamente más alto en Israel: el Estado judío posee una bien articulada red de instituciones que están dedicadas específicamente al combate en el ciberespacio y no sólo esto, han dedicado una gran cantidad de recursos al desarrollo de herramientas que les permita estar a la vanguardia en la materia. Si se acepta la autoría israelí en el ataque a las plantas de enriquecimiento de uranio iraní, estaríamos hablando de algo totalmente nuevo y revolucionario, jamás antes hecho, al menos no hay conocimiento público de un ataque similar.

La elaboración de ciberarmas requiere de un grado de desarrollo tecnológico bastante elevado, además de contar con la colaboración de personas increíblemente capacitadas. Programas como Stuxnet y Flame han dejado perplejos a compañías especialistas en seguridad informática de larga data, tales como Kasperysky y Symantec, por su código tan extremadamente complejo, que pone duda la real capacidad de las autoridades iraníes para combatir la infección. Algo mucho más preocupante es la posibilidad que existan otras de estas ciberarmas de este tipo causando estragos en el territorio iraní y que ni siquiera hayan sido detectadas, tal como fue el caso de Flame, del cual se cree estuvo trabajando a la sombra por más de dos años.

En cambio, el caso ruso es bastante elemental. Cuando se analizan sus actos de agresión en el ciberespacio parecen más actos vandálicos que verdaderos ataques en el sentido rigurosamente militar del término. El DDoS es la técnica habitual rusa, que consiste en el uso de una gran red de computadoras infectadas llamada Botnet, en donde cada uno de los ordenadores que hacen parte de esta red han sido previamente infectados con algún código malicioso, por lo general un troyano. Estos computadores reciben el nombre de zombies, ya que quedan bajo el control del hacker que está realizando el ataque, quien hace uso de su vasta red para realizar múltiples solicitudes a la página web que se desea deshabilitar; en consecuencia, entre mayor sea el tamaño del botnet, más rápido y efectivo será el ataque: la página no podrá soportar el enorme volumen de solicitudes por parte de todos los zombies y eventualmente

terminará colapsando (Maulini, s.f). Se trata de un ciberataque muy simple, habitualmente practicado por hacktivistas, su impacto suele ser mediático y un tanto psicologico más que efectivamente un ataque con connotaciones militares, tal y como se evidenció en el caso de Georgia.

La razón principal es que las agresiones no suelen tener mucha duración: cuando un ataque de estos se está tornando muy grave, la principal acción a tomar y quizás la única, es desconectar por completo el servidor y esperar hasta que el ataque cese, pero cuando este es prolongado en el tiempo, bien estructurado y con objetivos muy claros puede tener serias consecuencias. Tal y como quedó demostrado en Estonia, donde los DDoS fueron permanentes y duraron al menos tres semanas, tiempo durante el cual los medios de comunicación fueron bloqueados y los sistemas bancarios colapsaron; tiempo sin medios de comunicación y un sistema financiero tambaleante tiene graves consecuencias sociales y económicas para cualquier estado.

Los ciberataques atribuidos tanto a Rusia como a Israel nunca han sido reconocidos por estas naciones, pero parece bastante obvio que estos gobiernos siempre han estado involucrados directamente en su realización. Los ataques realizados a las centrales nucleares iraníes no pudieron haber sido realizados por un grupo de hackers sin vinculación estatal, ya que se requiere de una significativa base económica y de la reunión de expertos en la materia, eso sin mencionar el hecho que para inyectar el virus en las instalaciones se requirió de una infiltración física en las mismas, algo que sólo pudo haber sido llevado a cabo por una institución militar con alta experiencia en este tipo de operaciones.

Por el otro lado Rusia sí tiene una excelente coartada, como ya se ha dicho anteriormente: la naturaleza del ataque es tan simple que se puede atribuir a personas del común, que de hecho parece ser el *modus operandi* ruso para no dejar indicios, solo que es bastante sospechoso cuando se usa el mismo método para encubrir las elecciones más corruptas desde la caída de la URSS, un objetivo que sólo podría ser perseguido por el gobierno. Incluso también, cuando se mira el ataque a Estonia, se puede notar un alto grado de sincronía y planeación en los ataques, una estrategia casi militar; pero de nuevo esto son sólo conjeturas, nada de esto puede ser probado aún.

Referencias

1. Anónimo. (2010). *La guerra de Osetia del sur.* Recuperado de http://www.mundohistoria.org/temas_foro/historia-desde-la-guerra-fria-hasta-la-ultima-decada/la-guerra-osetia-del-sur
2. Arun, N. (2012). *No hay tregua en la ciberguerra.* Recuperado de http://news.bbc.co.uk/hi/spanish/science/newsid_7560000/7560462.stm
3. Criado, M. Á. (2010). *"Un Código de software es un arma, igual que un misil".* Recuperado de http://www.publico.es/ciencias/302347/un-codigo-de-software-es-un-arma-igual-que-un-misil
4. Euronews. (2011). *Rusia: Ciberataques contra medios digitales de la oposición.* Recuperado de http://es.euronews.com/2011/12/04/rusia-ciberataques-contra-medios-digitales-de-la-oposicion
5. Euronews. (2012). *El virus Flame abre nueva etapa en la ciberguerra.* Recuperado de http://es.euronews.com/2012/05/29/el-virus-flame-abre-nueva-etapa-en-la-ciberguerra/
6. Greenberg, A. (2012). *New Research Shows Flame Malware Was Almost Certainly A U.S. Or Israeli Creation.* Recuperado de http://www.forbes.com/sites/andygreenberg/2012/06/11/new-research-shows-flame-malware-was-almost-certainly-a-u-s-or-israeli-creation/
7. Hosenball, M. (2012). *EEUU e Israel desarrollaron virus Flame contra Irán: reporte.* Recuperado de http://lta.reuters.com/article/internetNews/idLTASIE85J00M20120620
8. Langner, R. (2011). *Cracking Stuxnet, a 21st-century cyber weapon.* Recuperado de http://www.ted.com/talks/lang/en/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html
9. Markoff, J. (2008). *Before the Gunfire, Cyberattacks.* Recuperado de http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&oref=slogin
10. Maulini, M. (s.f.). *¿Qué es un ataque de DDoS?* Recuperado de http://www.e-securing.com/novedad.aspx?id=57
11. Meshcheriakov, V. (2012). *Rusia crea una estrategia de ciberguerra.* Recuperado de http://rusiahoy.com/articles/2012/03/21/rusia_crea_una_estrategia_de_ciberguerra_16580.html
12. Ministerio de Defensa Nacional. (2009). *Ciberseguridad y ciberdefensa: una primera aproximación.* Recuperado de http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf
13. Reuters. (2011). *Israel lanza cibercomando contra ataques informáticos*. Recuperado de http://noticias.terra.com.co/internacional/medio-oriente/israel-lanza-cibercomando-contra-ataques-informaticos,5efff8e9e7300310VgnVCM20000099f154d0RCRD.html
14. Reuters. (2012). *Irán detecta "ciberataque masivo": TV.* Recuperado de http://lta.reuters.com/article/internetNews/idLTASIE85K0ED20120621?pageNumber=1&virtualBrandChannel=0
15. Reuters. (2012). *Virus Flame, nueva arma cibernética.* Recuperado de http://www.elcolombiano.com/BancoConocimiento/I/infografia_virus_flame_nueva_arma_cibernetica/infografia_virus_flame_nueva_arma_cibernetica.asp
16. Russia Today. (2012). *Los científicos advierten: una ciberguerra global sería igual que una atómica*. Recuperado de http://actualidad.rt.com/actualidad/view/47036-Los-cient%C3%ADficos-advierten-una-ciberguerra-global-ser%C3%ADa-igual-que-una-at%C3%B3mica
17. Soriano, J. (s.f.). *El Arte de la Guerra y sus cibercomandos.* Recuperado de http://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