ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

18/2014 21 febrero de 2014

*Eguskiñe Lejarza Illaro**

CIBERGUERRA, LOS ESCENARIOS DE CONFRONTACIÓN

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

CIBERGUERRA, LOS ESCENARIOS DE CONFRONTACIÓN

Resumen:

El desarrollo de internet en la década de los 90 delimita un antes y un después en el comportamiento socioeconómico mundial. El volumen de las operaciones llevadas a cabo en la red crecía paralelamente a las amenazas, hasta convertirse en un riesgo que comprometía la seguridad nacional. Nacía así el concepto de ciberarmas, programas destinados a infligir tales daños, que algunos han querido equiparar con las armas nucleares. El incremento en importancia de los ataques, la imposibilidad de adjudicar fehacientemente la autoría de los mismos y la carencia de repercusiones legales se unía a las consecuencias imprevisibles que podían ocasionar, obligando a los gobiernos a plantearse un doble debate: la defensa o el ataque contra un enemigo que se oculta en la "niebla de la red".

Abstract:

The development of Internet in the 90s delimits a before and after in the global socio-economic behavior. The volume of the operations carried out on the network growing in parallel with the threats, to become a risk that compromised national security. Thus was born the concept of cyber weapons, programs to inflict such harm, that some have tried to equate with nuclear weapons. The increased importance of the attacks, the inability to reliably assign the authorship of them and the lack of legal repercussions are bound to unpredictable consequences, forcing governments to consider a debate: defense or attack an enemy who is hidden in the "fog of the network".

Palabras clave:

Ciberguerra, ciberamenazas, infraestructuras críticas, espionaje, internet, virus informático.

Keywords:

Cyberwar, cyber threats, critical infrastructure, espionage, internet, computer viruses.

CIBERGUERRA, LOS NUEVOS ESCENARIOS DEL FUTURO

In an interconnected world, an attack on one nation's networks can be an attack on all."
Hillary Clinton
Secretary of State[1]

INTRODUCCIÓN

Hace poco más de 20 años el mundo entero participaba del prometedor desarrollo de la red global: la información podía ser conocida, gestionada y compartida instantáneamente desde cualquier punto del planeta gracias a un simple terminal, de una manera libre y gratuita. Las tecnologías de la información se convertían entonces en una herramienta imprescindible para las actividades económicas, sociales, empresariales, militares o de prestación de servicios, que comprobaban simultáneamente cómo éstas actividades se convertían en objetivos de la influencia maliciosa de virus, troyanos o gusanos que boicoteaban su seguridad.

La importancia creciente y el volumen de las operaciones llevadas a cabo en la red llevó implícita un acelerado aumento de las actividades ilícitas cometidas en ella: las primeras brechas de seguridad pronto derivaron en importantes amenazas, traducidas en robo de información sensible, que afecta a la soberanía y seguridad de las naciones, bloqueo de infraestructuras informáticas o espionaje industrial, con el fin de conocer las fortalezas de los competidores.

El control del ciberespacio fue tan controvertido en sus inicios como ha resultado ser cualquier intento de regulación de las actividades llevadas a cabo en él. Desde el principio, la figura del delincuente en la red ha evolucionado del hacker casi inofensivo a formados ciberdelincuentes movidos por fines económicos, políticos o sociales. Paralelamente a esta evolución, las herramientas utilizadas para infligir daño han crecido en sofisticación y potencia destructiva hasta el punto de que las consecuencias del empleo de ciberarmas está siendo comparado con las armas nucleares.

La aparición de un espacio virtual de interacción, al que se accede de manera inmediata y por un bajo coste, ha difuminado las fronteras existentes hasta el momento, modificando el comportamiento de defensa de los actores implicados ante el fantasma de un ataque de graves consecuencias cuya autoría, a pesar de las pruebas existentes, es difícilmente

[1] CNN, 21.01.2010, *Clinton: Internet "information curtain" is dropping*. Disponible en http://edition.cnn.com/2010/TECH/01/21/clinton.internet/. Fecha de la consulta 11.11.2013

imputable. El ciberespacio, tal como lo describe el MI5, comprende "los medios electrónicos de las redes digitales utilizados para almacenar, modificar y comunicar información. Incluye no solamente Internet, sino también otros sistemas de información que soportan las empresas, infraestructura y servicios. Todos dependemos de la disponibilidad de estos sistemas sobre una base diaria. Sin embargo, algunos individuos y grupos utilizan el ciberespacio con fines maliciosos. Llamamos a estas personas actores hostiles"[2].

La creciente conciencia sobre las ciberamenazas y la constante presencia de los citados actores hostiles en la red, bien sean gobiernos, empresas o delincuentes comunes, ha obligado a los países a replantearse las posibles vulnerabilidades de sus gobiernos ante las actividades ilícitas en la red**.** De hecho, el reconocimiento de la dependencia que los gobiernos tienen de la red, como fuente de información y escenario de actividades económicas y políticas, activó el instinto de defensa nacional en un medio tan vasto como difuso.

ESCENARIOS DE CIBERCONFLICTO

En 1996, el "National Defense Research Institute"[3] publicaba un estudio elaborado entre enero y junio del año anterior, en el que se auguraba ya que la estrategia de seguridad norteamericana se vería profundamente afectada por la rápida evolución del ciberespacio. El documento, bajo el epígrafe "Strategic Information Warfare. A New Face of War", ofrecía los resultados de un trabajo de investigación patrocinado por la Secretaria de Defensa norteamericana sobre dos cuestiones relevantes: evaluar los eventuales problemas de seguridad nacional que se desprenderían de la guerra de información estratégica, y establecer las posibles posturas defensivas que se podían adoptar ante ella[4].

La llamada Guerra de la Información (IW) ofrecía un perfil de rápida evolución impulsada por la todavía incipiente andadura de internet, los microordenadores y su asociación al imparable y vertiginoso desarrollo de la tecnología que hacía plantearse, ya hace casi 20 años, una conclusión básica: la obsolescencia de la estrategia militar nacional vigente ante las nuevas amenazas que plantearía la Guerra de Información Estratégica. Es por ello, que las

[2]MI5, The Threats: Cyber. Disponible en https://www.mi5.gov.uk/home/the-threats/cyber.html. Fecha de la consulta 18.11.2013.

[3] El "National Defense Research Institute", es un centro de investigación y desarrollo financiado por el gobierno federal de los EEUU, que lleva a cabo investigaciones de la RAND para la Oficina del Secretario de Defensa, el Estado Mayor Conjunto, los Mandos Conjuntos, las agencias de defensa, el Cuerpo de Marines y la Armada.
La RAND Corporation es una organización sin ánimo de lucro, dedicada a la investigación y el análisis, en campos tan diversos como la salud, los asuntos internacionales y la seguridad nacional entre otros. Para ampliar información consultar en www.rand.org .

[4] MOLANDER Roger C., RIDDILE Andrew S., WILSON Peter A., *Strategic Information Warfare A New Face of War*, Santa Monica, RAND, 1996, pág.1. Disponible en http://www.rand.org/pubs/monograph_reports/MR661.html. Fecha de la consulta 14.11.2013.

conclusiones del estudio firmado por Roger C. Molander, Andrew S. Riddile, Peter A. Wilson resultaron tan reveladoras en su momento como proféticas a la luz de lo acontecido dos décadas después.

Durante seis meses, más de 170 expertos en seguridad nacional, militar y otros ámbitos comprometidos en la guerra de la información, participaron en un ejercicio, cuya metodología, conocida como "The Day After" (El Día Después), había sido previamente utilizada en estudios relacionados con inteligencia y proliferación nuclear. Para el desarrollo del ejercicio, y ante la falta de experiencias previas en ataques con ciberarmas, se tomaron cuatro escenarios hipotéticos, sobre los que se aplicaron otros tantos supuestos conflictos que podrían motivar el uso delictivo del ciberespacio a nivel internacional:

- El Golfo Pérsico, con ataques promovidos por Irán y sus aliados domésticos contra otros países de la zona.
- China, que tras un hipotético intento de dominación regional y la declaración de independencia de Taiwán, iniciaría una contundente respuesta militar, la cual incluiría técnicas de guerra de la información, para disuadir a Estados Unidos de una posible injerencia militar.
- Rusia, en cuyo caso la hipótesis de trabajo presentaba una Federación nacional dirigida por un gobierno central débil y sometido a organizaciones de crimen transnacional, que no dudarían en hacer uso de técnicas de IW ofensivas y defensivas, para imponer sus objetivos frente a la oposición de Estados Unidos, varios estados miembros de la Unión Europea y el propio Gobierno ruso.
- La cuarta hipótesis del trabajo presenta a un México al borde de la segunda Revolución, profundamente desestabilizado por la rebelión de Chiapas.[5]

La Guerra de Información Estratégica, a pesar de la escasa experiencia que en ese momento se disponía sobre su devenir futuro, se presentaba como una modalidad de conflicto especialmente peligroso, al conllevar características diferenciales no apreciadas en ningún otro hasta el momento:

1. **Bajo coste de entrada:** Esto es, por el precio de un ordenador y una conexión a Internet, cualquier persona podría llevar a cabo acciones de ciberguerra, bien sean actores individuales o ciberejércitos, con un objetivo concreto.
2. **Las fronteras tradicionales se hacen borrosas**: La ciberguerra crea su propia "Niebla de Guerra". Sin la existencia de límites claros, la distinción entre intereses públicos y privados quedaría comprometida, a la vez que el carácter abierto de la red favorecería la proliferación de posibles organizaciones atacantes y de herramientas de ataque. Todo

[5] Ibíd., pág. 6.

ello sin que pudiera diferenciarse, a priori y con facilidad, cuales provienen del mismo territorio y cuales son acciones hostiles contra el país, lo que provocaría una escalada de ambigüedades y susceptibilidades entre gobiernos.

3. **Ampliación del papel de la gestión de la percepción:** Referida a la capacidad de manipulación de la información, así como a la alteración de archivos multimedia por parte de actores hostiles al gobierno, con la finalidad de manipular cualquier acción o decisión adoptada por éste, limitando así su capacidad para mantener apoyos ante acciones polémicas.
4. **Deficiente inteligencia estratégica:** Se alertaba que los métodos de inteligencia tradicional, y sus consiguientes análisis, resultan obsoletos en el escenario actual. El ciberespacio dota al enemigo de una libertad y rapidez de acción inusual hasta el momento, por lo que el peso de la amenaza tiene que ser evaluada en función de las capacidades del atacante, sus intenciones y la vulnerabilidad que se detecte en su objetivo.

   El informe concluye que será extremadamente difícil para la comunidad de inteligencia desarrollar y mantener una lista estable de amenazas potenciales. El entorno global se ha movido a una multipolaridad mucho más dinámica, en contraposición a la estructura bipolar estática de antaño. "Dependiendo de las circunstancias geoestratégicas y económicas, el Gobierno de Estados Unidos puede encontrarse a uno o más de sus tradicionales aliados actuando como rivales económicos"[6], por lo que "la Inteligencia estratégica se encuentra con el problema de identificar al adversario, sus capacidades e intenciones"[7].
5. **Dificultad de alerta táctica y evaluación del ataque:** La facilidad con la que el adversario puede acceder a un ciberarma, crea la imposibilidad de conocer de antemano el inicio de la ofensiva , así como de predecir la magnitud de la misma. El carácter anónimo del ciberespacio dificulta conocer la autoría y el método utilizado en el ataque, hechos ambos que determinan que el autor se vea inicialmente favorecido.
6. **Dificultad para el establecimiento y mantenimiento de coaliciones con otros países:** Referido al caso concreto de Estados Unidos, se incide en la necesidad de que los eventuales socios de una coalición cumplan unas condiciones de desarrollo tecnológico, ya que las vulnerabilidades asimétricas exacerbarían el problema. Además, el gobierno debe asegurarse de que estos aliados no sean objetivos potenciales de ciberataques.
7. El último punto está referido concretamente a la presumible vulnerabilidad de Estados Unidos ante la evidencia de la Guerra de Información Estratégica, avalada por el progresivo aumento de la dependencia que este país tendría en el futuro de los sistemas de información.

[6] Ibíd., pág. 25.
[7] Ibíd., pág. 25.

La amenaza persistente y anónima de un ciberataque inauguraba un nuevo escenario de confrontación y defensa: el ciberespacio. Esto suponía un salto cualitativamente sustancial en diversas vertientes: los ataques y la magnitud de sus consecuencias son difícilmente predecibles, la "niebla" del ciberespacio desdibuja el perfil del autor cuya identidad, aunque presuntamente conocida, es difícilmente demostrable y, por último, las normas de confrontación en este nuevo escenario y las consecuencias legales son igualmente difusas.

Michael Chertoff, ex Secretario estadounidense de Seguridad Nacional confirmaba, durante la III Edición del "World Cyberspace Cooperation Summit", que las conclusiones del estudio de 1995 no podían ser más certeras: "Lo que hemos aprendido a lo largo de los últimos 10 o 20 años, es que no puedes asumir confianza. Esto se debe a que estamos tratando con un persistente problema de criminalidad, robo de propiedad intelectual e incluso esfuerzos para sabotear o dañar nuestras infraestructuras utilizando Internet"[8].

El avance de las amenazas y la proliferación de ciberarmas con propósitos destructivos, han modificado los parámetros de defensa convencionales y provocado de una manera inherente movimientos sustanciales en el comportamiento de los actores políticos, económicos y militares de las naciones ante un enemigo que se confina en la red. El ciberespacio no solo transformaba la forma de relación política y económica mundial, sino que fijaba una nueva frontera en todos los ámbitos existentes, creando así una nueva encrucijada para la seguridad nacional.

Había nacido un nuevo dominio en el que incluso era difícil determinar qué constituye un ataque y qué no, donde acaban los actos de espionaje o intrusiones malintencionadas y dónde empieza lo que puede definirse como un acto de guerra. En última instancia, la evaluación del ataque y su calificación final, recae únicamente en el criterio político de la nación destinataria.

Ante la situación actual, el exsecretario adjunto de Defensa, William Lynn afirmó en 2010 que "por una cuestión de Doctrina, el Pentágono ha reconocido formalmente el ciberespacio como un nuevo dominio de guerra. Aunque sea un dominio hecho por el hombre, se ha convertido en algo tan crítico para las operaciones militares como la tierra, el mar y el aire"[9]. Para William Lynn, las ciberarmas no conllevan las implicaciones existenciales que marcaron el comienzo de la era nuclear, pero "existen importantes similitudes. Este tipo de ataques puede no causar las bajas masivas de un ataque nuclear, pero igualmente podrían paralizar a

[8] Cybersummit 2013, Act of Aggresion in Cyberspace. Disponible en http://cybersummit.info/topics/acts-aggression-cyberspace . Fecha de la consulta 19.11.2013.
[9] WILLIAM J. Lynn III, "Defending a New Domain", Foreign *Affairs,* de 1 de septiembre de 2010. Disponible en http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain. Fecha de la consulta 15.12.2013.

la sociedad estadounidense"[10].

Dos años más tarde, el Secretario de Defensa Norteamericano, Leon Panetta, certificaba su creencia de que los ciberataques eran tan reales como otras amenazas ya conocidas como "el terrorismo, la proliferación de armas nucleares o la agitación que vemos en Oriente Medio"[11]. Panetta describía los escenarios más destructivos como aquéllos que "involucran a ciberactores lanzando varios ataques al mismo tiempo contra nuestras infraestructuras críticas, en combinación con un ataque físico en nuestro país. Los atacantes también podrían buscar desactivar o degradar los sistemas militares y redes de comunicaciones. El resultado colectivo de este tipo de ataques podría ser un ciber Pearl Harbor, que causaría la destrucción física y la pérdida de vidas, un ataque que paralizaría y dejaría en shock a la nación, y crearía un nuevo sentido profundo de vulnerabilidad"[12].

La creciente conciencia sobre las vulnerabilidades y brechas de seguridad de los países ha sido objeto de numerosos estudios, cuya pretensión era dibujar el mapa de ruta de un ciberataque y definir posibles vulnerabilidades. En esta dirección, Forward presentaba en 2010 el Libro Blanco de las Amenazas Emergentes[13], en el que se discutía las posibles ciberamenazas y las áreas en las que éstas podrían materializarse. Para ello se exponen diez ciberamenazas previsibles que se aplican sobre otros tantos hipotéticos escenarios, con el fin de demostrar cómo ciertas vulnerabilidades pueden ser aprovechadas con fines maliciosos. Asimismo, se refiere a las previsibles las consecuencias sociales, económicas y medioambientales que ellas provocarían.

Los escenarios críticos, en cuya identificación participaron expertos informáticos y miembros de organizaciones industriales y gubernamentales fueron los siguientes:

1. Fraude electoral.
2. Espionaje Industrial.
3. Ruptura del mercado de valores por beneficio o diversión.
4. Espionaje industrial
5. Provocar derrames intencionados de petróleo.
6. Toma del control de la fabricación.

[10] Ibíd.
[11] Palabras del Secretario de Defensa de los EEUU, Leon Panetta sobre ciberseguridad a ejecutivos de empresas para la Seguridad Nacional en la ciudad de Nueva York el 11 de octubre de 2012. Disponible en http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136. Fecha de la Consulta 09.12.2013.
[12] Ibíd.
[13] *White Book: Emerging Information & Communication Technologies threats*, FORWARD Consortium, 17 de enero de 2010. Disponible en http://www.ict-forward.eu/media/publications/forward-whitebook.pdf . Fecha de la consulta 22.11.2013.

7. Comprometer el Smartphone de un político.
8. Chantaje masivo a través de las redes sociales.
9. Ataque contra una central eléctrica.
10. Ataque contra una central hidroeléctrica.

EVOLUCION DE LAS CIBERAMENAZAS

Los vaticinios del trabajo de 1995 de Molander, Riddile y Wilson no tardaron muchos años en cumplirse. Las actividades en la red iniciaron una escalada que modificó el rumbo de la historia.

1999, Guerra de Kosovo. El Capitán Dragan, héroe nacional serbio durante la Guerra de Krajina (Croacia), encabeza un ejército de más 450 voluntarios compuesto por expertos informáticos de varias naciones que se enfrentaron a los aliados. La misión del grupo no es otra que romper el bloqueo informativo impuesto por el enemigo y lanzar al mundo su propia visión de la guerra. Piratas informáticos rusos y alemanes, acudieron a la llamada de ayuda de Dragan. El grupo, que manejaba cuarenta ordenadores, instalados en un rascacielos, consiguió bloquear durante un fin de semana la web de la Casa Blanca e infiltrarse en los sistemas informáticos de la OTAN y el portaviones norteamericano Nimitz[14].

1998-2000, Operación Moonlight Maze. Es una de las operaciones informáticas más grandes conocidas. Durante dos años, hackers saquearon datos procedentes de los ordenadores del Pentágono, la NASA, Universidades y centros de investigación norteamericanos, así como del Departamento de Energía, accediendo a miles de documentos de relevancia nacional. Aunque nunca se llegó a probar la autoría, las investigaciones apuntaron a piratas informáticos que operaban desde Rusia. El Gobierno Ruso negó cualquier patrocinio en esta actividad[15].

En el 2005, The Washington Post hace pública la denuncia de un ataque, presuntamente responsabilidad de China, que recibió el nombre de Operación Titán. En esta ocasión, los destinatarios del ataque eran las redes de los Departamentos de Defensa, Estado, y Energía así como contratistas de Defensa[16]. Un informe del "Congressional Research Service" reconocía que este ataque, junto con Moonlight Maze "son ejemplos de ataques exitosos

[14] El Mundo, Guerra informática en Serbia, 26 de abril de 1999. Disponible en http://www.elmundo.es/navegante/99/abril/16/hackers.html. Fecha de la consulta 19.11.2013.
[15] Congressional Research Service, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, 27 de marzo de 2007, pág. 10. Disponible en http://www.fas.org/sgp/crs/natsec/RL31787.pdf . Fecha de la consulta 15.12.2013.
[16] The Washington Post, Hackers Attack Via Chinese Web Sites, 25 de Agosto de 2005. Disponible en http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html . Fecha de la consulta 26.11.2013.

contra los sistemas militares no clasificados, y que según Oficiales de Defensa eran dirigidos por otros gobiernos"[17]. El informe concluye además que potenciales enemigos de Estados Unidos como China, Rusia, Cuba, Irán, Iraq, Libia o Corea del Norte, además de múltiples grupos terroristas no estatales, disponían de capacidades para atacar las redes civiles y militares norteamericanas.

En el 2010, de nuevo The Washington Post publicaba datos sobre una vasta campaña de ciberespionaje chino contra los sistemas informáticos de, al menos, 34 importantes compañías estadounidenses. Los expertos señalaron entonces la aparición de un nuevo nivel de sofisticación del ataque, que utilizaba diversos tipos de códigos maliciosos. La denominada Operación Aurora tenía como supuesta finalidad el espionaje industrial y el contraespionaje[18].

La complejidad y capacidad destructivas de las ciberarmas se ha perfeccionado progresivamente hasta llegar a la relevancia del célebre Stuxnet, pionero en el uso de códigos maliciosos altamente sofisticados en ataques dirigidos contra importantes instalaciones industriales, como plantas de energía eléctrica o sistemas de procesamiento de deshechos. La compañía de Seguridad Informática Symantec, califica a Stuxnet como "el primer virus informático que permite hacer daño en el mundo físico"[19].

El presunto objetivo del malware era destruir las centrifugadoras nucleares iraníes de Natanz, que permiten el enriquecimiento de uranio, evitando así la fabricación de armamento atómico por parte de este país. Un informe publicado por el New York Times revela que el ataque fue un éxito y que llegó a destruir cerca de 1.000 centrifugadoras, una sexta parte del total que el gobierno de Teherán poseía entonces. La propagación del gusano, pudo retrasar hasta en dos años el programa nuclear de Irán[20].

A pesar de que el informe publicado por este rotativo adjudicaba la autoría y posibles motivos para la puesta en marcha de esta ciberarma, lo cierto es que es imposible determinarlo de una manera fehaciente. Un informe elaborado por Symantec, revelaba que la compleja arquitectura funcional del gusano requería de muchas y diferentes habilidades para su puesta en marcha, así como una gran organización y medios económicos. "Realmente nunca hemos visto algo así antes y el hecho de que pueda controlar el

[17] Congressional Research Service, Op. cit., pág. 10.
[18] The Washington Post, Google China cyberattack part of vast espionage campaign experts say, 14 de enero de 2010. Disponible en http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html . Fecha de la consulta 24.11.2013.
[19] Symantec, La importancia de Stuxnet, disponible en http://www.symantec.com/es/es/outbreak/?id=stuxnet. Fecha de la consulta 11.12.2013.
[20] The New York Times, Malware Aimed at Iran Hit Five Sites, Report Says, 11 de febrero de 2011. Disponible en http://www.nytimes.com/2011/02/13/science/13stuxnet.html?_r=0 . Fecha de la consulta 22.11.2013.

funcionamiento de una maquinaria física es inquietante"[21], según Liam O'Murchu, investigador de Symantec Security Response.

Pero Irán no fue la única víctima, aunque sí la más perjudicada, por la actividad del gusano. Según Symantec, de los 100.000 ordenadores afectados, casi 60.000 se encontrarían en este país; el resto se repartiría, por orden de importancia, entre Indonesia, India, Azerbaiyán, Pakistán y Malasia. En menor medida, el informe apunta que también fueron infectados ordenadores de Estados Unidos, Uzbekistán, Rusia y Gran Bretaña[22].

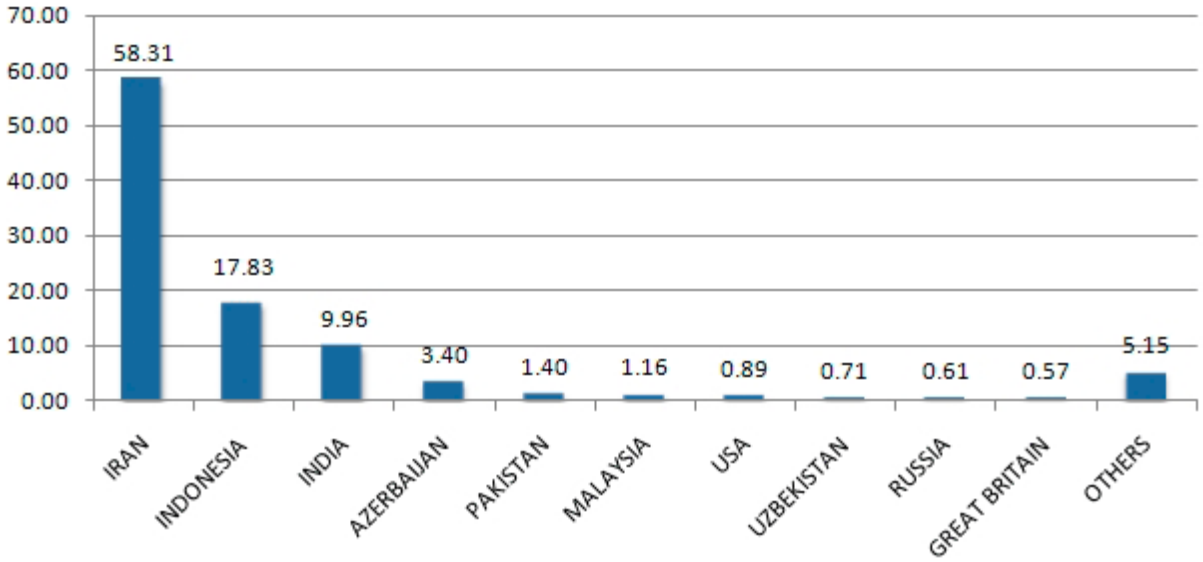

Figura 1: Distribución Geográfica de la Infección por Stuxnet.
Fuente: Symantec[23].

Stuxnet tuvo en el virus Duqu un digno sucesor, de autoría también desconocida, y cuya máxima potencialidad consistía en atacar sistemas informáticos industriales, disfrazándose de documento Word. Irán volvía a ser el objetivo de esta nueva ciberarma, que también fue detectada en Sudán, Francia, India, Suiza o Ucrania. Según Kaspersky, ambos virus jugaron un notable papel en las ciberbatallas que se libran en Oriente Medio.[24]

A mediados del 2012, los expertos en seguridad de Kaspersky fueron requeridos por la Unión Internacional de Telecomunicaciones (UIT), dependiente de la ONU, para encontrar un programa malicioso que robaba información confidencial de países de Oriente Medio.

[21] Symantec, El gusano Stuxnet. Disponible en http://www.symantec.com/es/mx/theme.jsp?themeid=stuxnet. Fecha dela consulta 10.12.2013.
[22] Symantec, W32.Stuxnet Dossier Versión 1.4, 11 de febrero de 2011. Disponible en http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Fecha de la consulta 11.12.2013.
[23] Ibíd.
[24] Kaspersky, Flame: preguntas y respuestas, 30 de mayo de 2012. Disponible en http://www.viruslist.com/sp/weblog?weblogid=208188630. Fecha de la consulta 03.12.2013.

Durante la búsqueda de este Código, apodado Wiper, descubrieron la siguiente y sofisticada ciberama, el "Worm.Win32.Flame"[25].

La novedad de Flame radica esencialmente en su complejidad. Se trata de un sofisticado paquete de herramientas que, según las investigaciones se instalaba a través de ataques dirigidos. Una vez infectado el sistema, comenzaba una compleja serie de operaciones, como la intercepción del tráfico de red, capturas de pantalla, grabación de conversaciones orales y la intercepción del teclado entre otras. Todos estos datos se ponen a disposición de los dueños de Flame a través del enlace a sus servidores. Su finalidad era la obtención sistemática de datos sobre las operaciones llevadas a cabo en Oriente Medio por Irán, Israel, Palestina, Sudán, Siria, Líbano, Arabia Saudí y Egipto, que fueron, por orden de importancia y número de ataques, los países afectados.

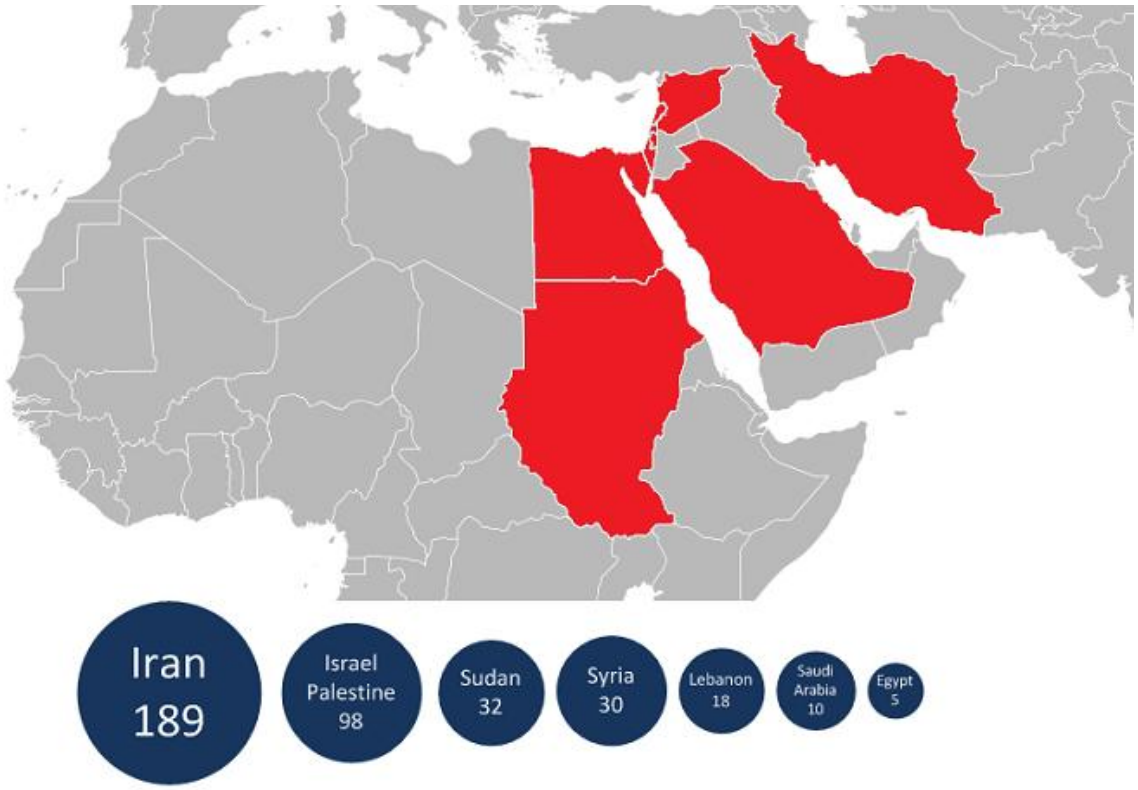

Figura 2: Países afectados por Flame.
Fuente: Kaspersky Lab[26].

Flame no pudo ser vinculado a ningún gobierno, por lo que, al igual que en los casos de Stuxnet y Duqu, la autoría quedo en el anonimato.

[25] Ibíd.
[26] Ibíd.

No pasó mucho tiempo, hasta que Oriente Medio volvió a ser el objetivo del último protagonista de la destructiva saga de ciberarmas protagonizada por los tres anteriores. En esta ocasión se trataba de un troyano bancario dirigido al ciberespionaje gubernamental llamado Gauss, cuya habilidad para robar credenciales online de bancos, "era algo que no habíamos visto antes en ataques de malware patrocinados por un gobierno"[27], asegura Kaspersky. Según la compañía de seguridad, la mayoría de las víctimas de Gauss se encuentran en Líbano. También hay víctimas en Israel y Palestina, Estados Unidos, los Emiratos Árabes Unidos, Qatar, Jordania, Alemania y Egipto.

LOS CIBERATACANTES

Para la Compañía de Seguridad Kaspersky, no hay lugar a la duda. "Hoy en día hay tres tipos conocidos de actores que desarrollan programas maliciosos y programas espía: los hacktivistas, los ciberdelincuentes y los gobiernos. Flame no está diseñado para robar dinero desde cuentas bancarias. Difiere además de los sencillos programas maliciosos y herramientas de ataque que usan los hacktivistas. Entonces, excluyendo a los ciberdelincuentes y a los hacktivistas, llegamos a la conclusión de que pertenece al tercer grupo"[28]. Kaspersky incide además en que la disposición geográfica de los blancos alcanzados por este ciberarma, la mayoría ubicados en Oriente Medio "no dejan dudas de que sea un gobierno quien ha financiado toda la investigación necesaria para su desarrollo"[29].

"Hay suficientes evidencias como para afirmar que tiene una relación muy cercana con Flame y Stuxnet, que son ataques patrocinados por un estado o nación. Tenemos pruebas de que Gauss se creó en la misma "fábrica" (o fábricas) que produjeron Stuxnet, Duqu y Flame. Observando a los cuatro, podemos explicar la relación que existe entre ellos"[30].

[27] Kaspersky, Gauss: Troyano bancario se utiliza en el espionaje cibernético gubernamental, 13 de agosto de 2012. Disponible en http://www.viruslist.com/sp/weblog?weblogid=208188666. Fecha de la consulta 03.12.2013.
[28] Kaspersky, Flame: preguntas y respuestas, Op. cit.
[29] Ibíd.
[30] Kaspersky, Gauss: Troyano bancario se utiliza en el espionaje cibernético gubernamental, Op. cit.

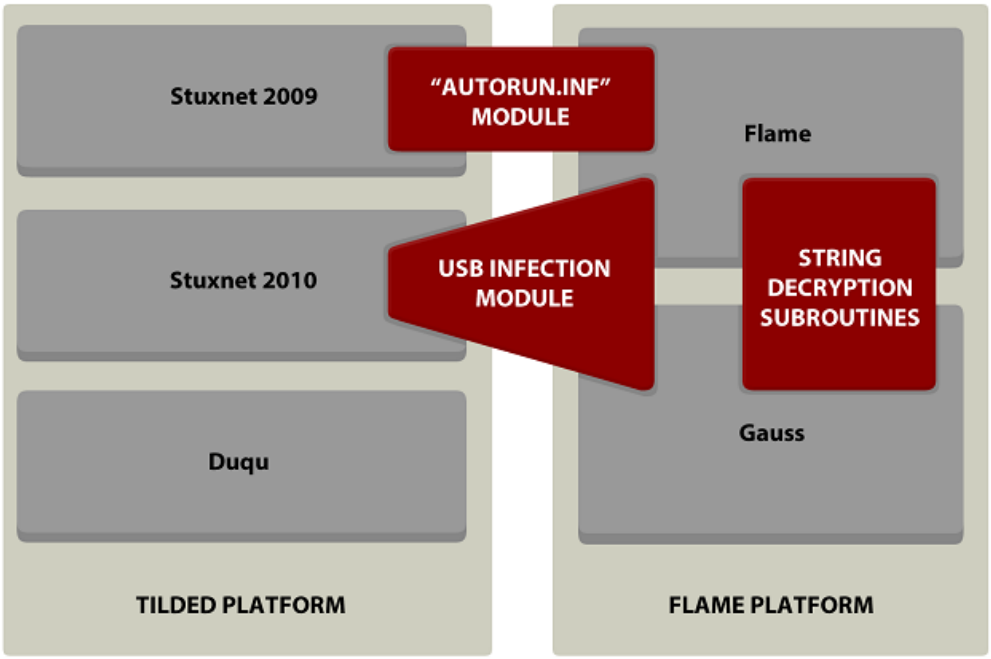

Figura 3: La relación de Stuxnet, Duqu, Flame y Gauss.
Fuente: Kaspersky Lab[31].

Pero además de los objetivos de estos cuatro virus, han sido muchos otros los países que han denunciado ataques a sus redes informáticas, bien destinadas al robo, o bien al bloqueo de sus infraestructuras críticas. En 2011, McAfee hacía público el informe llamado "Operación Shady RAT"[32] que, firmado por su vicepresidente, Dimitri Alperovitch, pretendía demostrar que más de 70 compañías, gobiernos y organizaciones sin ánimo de lucro habían sido víctimas de intrusiones durante los últimos cinco años. Según, el informe, los ciberdelincuentes habían fijado ataques en objetivos de catorce países: Estados Unidos, Canadá, Corea del Sur, Taiwán, Japón, Suiza, Reino Unido, Indonesia, Vietnam, Dinamarca, Singapur, Hong-Kong, Alemania e India[33].

Alperovitch advertía que lo más sorpréndete es la diversidad de las víctimas y la audacia de los ciberdelincuentes, e incide en la relevancia de que "prácticamente todo el mundo está cayendo presa de estas intrusiones, independientemente de que sean las Naciones Unidas, una empresa multinacional, un pequeño think tank sin ánimo de lucro, un equipo olímpico nacional e incluso una desafortunada firma de seguridad"[34].

"Lo que hemos presenciado durante estos cinco o seis años ha sido nada menos que una

[31] Ibíd.
[32] RAT es un acrónimo común en la industria, que es sinónimo de herramienta de acceso remoto.
[33] McAfee, Revealed: Operation Shady Rat, 2011. Disponible en http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf . Fecha de la consulta 02.12.2013.
[34] Ibíd., pág. 3.

transferencia de riqueza sin precedentes, secretos nacionales celosamente guardados, códigos fuente, bases de datos, archivos de correo electrónico, planes de negociación y explotación de nuevos campos de petróleo y gas, contratos legales y mucho más"[35]. La importancia económica, política y estratégica de la información sustraída sería tal que Alperovitch llegó a afirmar que la totalidad de las compañías incluidas en la lista "Fortune Global 2000"[36] podían incluirse en dos categorías: "las que han sido comprometidas y aquéllas que aún no lo saben"[37].

Los registros efectuados por McAfee ofrecen un panorama sorprendente, si se observan los emplazamientos de las organizaciones seleccionadas y la diversidad de las actividades que realizan en los diversos ámbitos económicos, políticos, sociales y culturales.

- En 2006, el año en que empiezan los registros, se computan sólo ocho: Las víctimas son empresas de acero y construcción de Corea del Sur, una firma de bienes raíces de Estados Unidos, organizaciones de comercio internacional asiáticas y occidentales y la Secretaría de la ASEAN[38].
- En 2007, el ritmo de actividad crece en un 260%, hasta contabilizarse un total de 29 víctimas. Se registran ataques a cuatro contratistas de defensa de Estados Unidos, a una compañía tecnológica propiedad del gobierno de Vietnam, varios organismos estatales de Estados Unidos, los Comités Olímpicos de las naciones asiáticas y occidentales.
- En 2008, la cuenta subió a 36 víctimas, incluyendo las Naciones Unidas y la Agencia Mundial Antidopaje, y en 2009 se contabilizan 38.
- El número de intrusiones cae a 17 en 2010 y a 9 en 2011. El motivo barajado por McAfee para este descenso fue probablemente debido a la adopción generalizada de medidas destinadas a contrarrestar las acciones de este atacante en concreto. Como en ocasiones anteriores, el informe concluye que fue imposible señalar, más allá de la simple sospecha, a un actor concreto tras los ataques.

La urgente necesidad por identificar en el mínimo plazo posible que se está siendo víctima de un ciberataque se revela como fundamental para contrarrestar sus efectos. Movidos por esta necesidad se han desarrollado sofisticadas herramientas para detectar los ataques en el ciberespacio. Una de ellas, el Mapa Digital de Ataque, permite visualizar en tiempo real las actividades de Denegación de Servicios que ocurre en todo el planeta. Esta monitorización es

[35] Ibíd., pág. 2.
[36] La lista de las compañías incluidas en Fortune Global 200 se puede consultar en http://www.forbes.com/lists/2006/18/06f2000_The-Forbes-2000_Rank.html. Fecha de la consulta 02.12.2013.
[37] McAfee, Op. cit., pág. 2.
[38] ASEAN es la asociación de Naciones del Sudeste Asiático. Más información en http://www.aseansec.org/ .

posible gracias a los datos recopilados por Arbor Network[39] y su colaboración con Google Ideas. El mapa permite observar el comportamiento de los ataques en tiempo real, el país de origen y el de destino, la duración y el ancho de banda ocupado, pero no desvela la identidad del atacante.

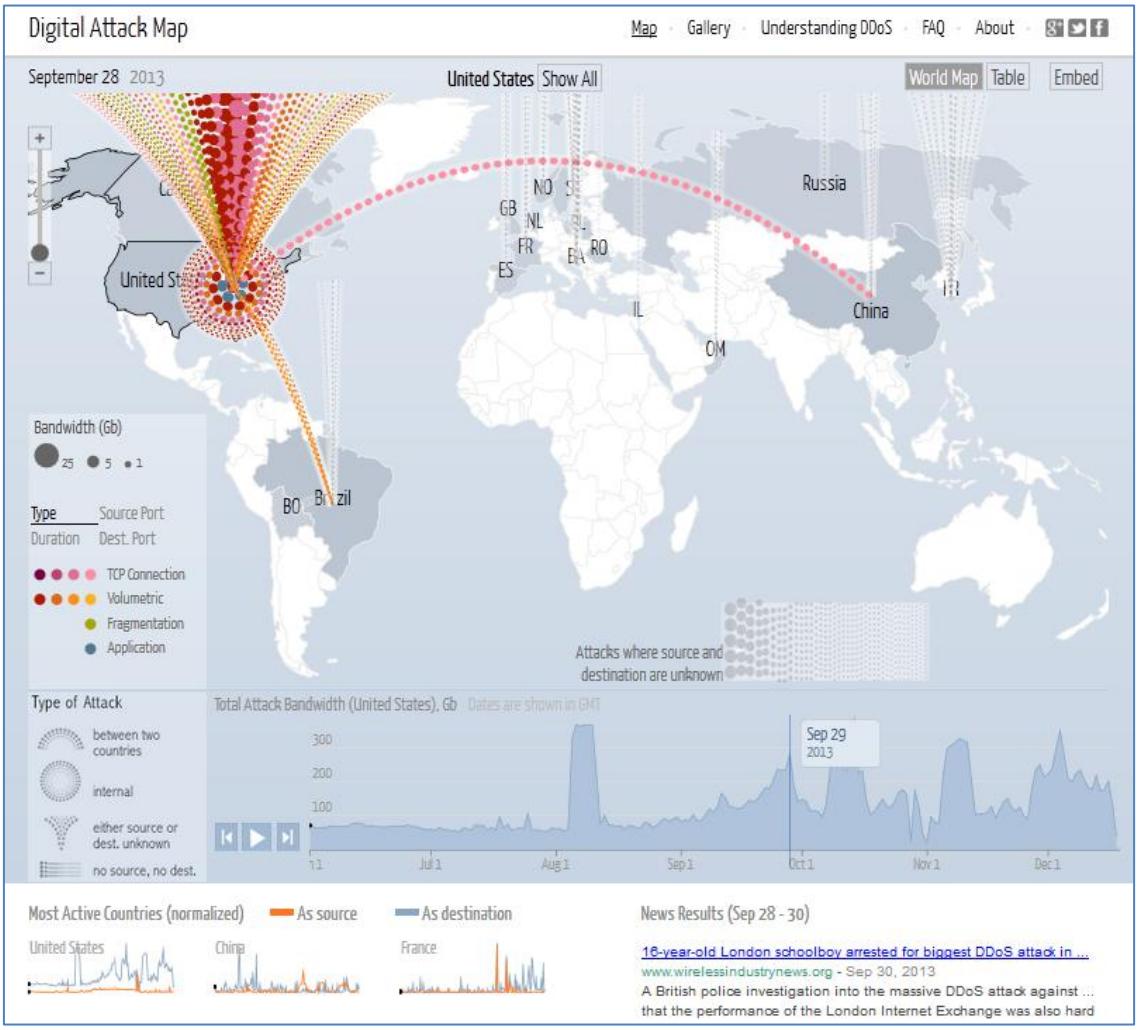

Figura 4: Mapa Digital de Ataque.
Fuente: Digital Map Attack[40].

En un intento por perfilar la identidad del atacante, Alberto Calvo, director de Sistemas de Seguridad de Indra, distingue cuatro perfiles en los atacantes:

- Ciberdelincuentes y Mafias: con el chantaje económico como medida de presión, estos actores amenazarían con difamar o destruir datos de sus víctimas, o bien los sustraerían con la intención de venderlos en el mercado negro.

[39] Para ampliar información sobre ARBOR Network consultar https://atlas.arbor.net/ .
[40] Disponible en http://www.digitalattackmap.com/about/ . Fecha de la consulta 17.12.2013.

- Ciberterroristas: que actuarían tanto para financiarse como para fines de propaganda o causar pérdidas en las instituciones e infraestructuras críticas de los países que consideran sus enemigos.
- Ciberactivistas: se tratarían de grupos antisistema, y la finalidad de las acciones sería desacreditar a aquellas instituciones contra las que actúan, con el fin último de modificar su comportamiento[41].
- Ciberejércitos: con "una capacidad financiera muy superior a los atacantes habituales" así como "una sofisticación máxima"[42].

El perfil también sufre una variación sustancial a lo largo de 35 años de actividad. Así se pueden identificar cuatro etapas diferenciadas:

1) Desde 1980 hasta el 2000, dominada por hackers motivados por la curiosidad, pero la mayoría benignos.
1) Del 2000 al 2005: esta segunda etapa estaría protagonizada por los "script kiddies", se trata de personas inexpertas, que utilizan herramientas informáticas elaboradas por otros, con la finalidad de intentar causar daños y hacerse famosos, pero sin objetivos claros.
2) Del 2005 al 2010, entraron en escena los cibercriminales, que utilizarían phishing, malware, bots con finalidades comerciales.
3) Del 2010 hasta la actualidad, el perfil de actor hostil evolucionaría hacia "profesionales, equipos de ciberguerra, mafias o hacktivistas a los que moverían ya objetivos políticos o estratégicos"[43].

Esta vuelta de tuerca en el perfil y objetivos de los atacantes ha contribuido a acuñar el término de guerra asimétrica: aunque la amenaza del ataque esté latente, la autoría y magnitud de la misma es casi siempre difusa, lo que provoca dudas sobre la proporcionalidad de las respuestas.

La autoría del ciberataque, la capacidad de destrucción o de bloqueo de servicios críticos, así como la respuesta que éste provoque, tanto a efectos paliativos como de defensa por parte del destinatario, ha sido y es objeto de distintas reacciones por parte de los gobiernos.

En el 2004, el Teniente Coronel Timothy O´Hara, publicaba un trabajo en el U.S. Army War College, bajo el título Cyber Warfare/Cyber Terrorism, en el cual explicaba que la ciberguerra

[41] Un ejemplo de ello sería el grupo hacktivista Anonymous, surgido en 2003, y que materializa sus protestas bloqueando las páginas web de aquellos organismos o instituciones contra los que dirige sus protestas con técnicas de hacker.
[42] Conferencia impartida por Luis Alberto Calvo, Director de Sistemas de Seguridad de Indra, el 22 de octubre de 2013, en el Encuentro Internacional de Seguridad de la Información (ENISE), que tuvo lugar en León (España). Disponible en http://www.7enise.webcastlive.es/. Fecha de la consulta 13.12.2013.
[43] Ibid.

se había convertido en la protagonista de los ataques no cinéticos de los enemigos de su país y su posible respuesta podría abarcar también un ataque convencional sobre el agresor.

"Nuestras recientes victorias militares, especialmente después de nuestros esfuerzos en la guerra del Golfo, demuestran claramente a quienes les gustaría hacernos daño que nosotros no podemos ser atacados con éxito a la manera tradicional en el ámbito político, económico y militar. Nuestros adversarios, conscientes de ello, entienden que la única oportunidad para lograr sus objetivos políticos, sociales o económicos se basa en la capacidad de atacarnos a través de la guerra por otros medios (WBOM. Warfare by Other Means)" [44]

En el concepto de WBOM del que habla el Teniente Coronel O'Hara, y dentro de la categoría de ataques cinéticos, un ciberataque podría llevarse a cabo con la finalidad de provocar efectos destructivos por sí mismo[45], o "bien como facilitador de un ataque convencional[46], que sería el que directamente provocaría la destrucción"[47].

"En el caso de un ataque no cinético, este no estaría dirigido a la destrucción física, sino que pretendería afectar a la voluntad de luchar del adversario y a su capacidad para tomar decisiones. Tradicionalmente, esta forma de guerra es la campaña de propaganda o desinformación. La Ciberguerra es ahora un herramienta primordial en el arsenal de la guerra de la Información para lograr ataques no cinéticos".

LAS CIBERARMAS Y LAS CONSECUENCIAS DE SU EMPLEO

Stuxnet, Duqu y Flame demostraron al mundo, en opinión de Eugene Kaspersky[48], que las ciberarmas son:

- Eficaces.
- Mucho más baratas que las armas tradicionales.
- Difíciles de detectar.
- Difícil de atribuir a un atacante particular.

[44] O'HARA Timothy F., *Cyber Warfare/Cyber Terrorism*, Carlisle, U.S. Army War College, 2004, pág. 3.
[45] Este sería el caso del virus Stuxnet.
[46] Un ejemplo de este tipo de ciberataque sería la introducción de un malware en la red de defensa aérea enemiga, para degradar su capacidad, y que facilite las incursiones aéreas propias.
[47] Conferencia "Ciberguerra, Temor, Incertidumbre y Duda", impartida por Roldán Fabián Garzón, el 30 de septiembre de 2013, durante la Conferencia Latinoamericana CACS/ISRM, que tuvo lugar en Medellín (Colombia). Disponible en http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/133.pdf . Fecha de la consulta 01.12.2013.
[48] KASPERSKY Eugene, The Flame That Changed the World, 14 de junio de 2012. Disponible en http://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-the-world/#more-2717. Fecha de la consulta 29.11.2013.

- Difíciles de protegerse contra ellas, teniendo en cuenta todas las vulnerabilidades de software desconocida.

Kaspersky alerta de la falta de cualquier tipo de Convención Internacional (es decir, un acuerdo respecto a las "reglas del juego") sobre el desarrollo, implementación y distribución de ciberarmas, para evitar que se conviertan en amenazas muy reales. Según su criterio, en términos de potencial destructivo, las ciberarmas "no son de ninguna manera inferiores a las armas nucleares, biológicas o químicas. Pero, a diferencia de estas armas de destrucción masiva, no están sujetas a ningún tipo de control y tienen el 'glamour' de ser invisibles, omnipresentes y precisas". Se remonta a la experiencia pionera de Stuxnet sobre el uso de programas maliciosos dirigidos contra instalaciones industriales, para ratificar que éste no fue un hecho aislado y augurar que "estamos en el umbral de una era de 'ciberguerra fría', en la que las naciones poseen la habilidad de librar batallas sin las limitaciones de la guerra convencional en el mundo real"[49].

La potencialidad destructiva de las ciberarmas y su impacto en las líneas defensivas de los países y las infraestructuras críticas, ha sido comparada con el conflicto político y moral que supuso la proliferación de las armas nucleares como parte de la tecnología militar. Para R. Scott Kemp, Profesor de Ingeniería y Ciencia Nuclear de la Universidad de Princeton:

> "Casi 70 años más tarde, nos encontramos en la misma disyuntiva con la ciberguerra. Las ciberarmas no parecen ser capaces de provocar una destrucción en masa, en el sentido que claramente lo son las armas nucleares, pero mantienen en riesgo algunos de los activos más preciados de nuestro tiempo: los mecanismos de almacenamiento y control de información sobre la cual se ha construido la sociedad moderna. No es difícil imaginar escenarios catastróficos como la destrucción de un sector bancario, la eliminación de un mercado de valores, la inundación de una presa, o el envenenamiento de un suministro de agua, todo iniciado por anomalías inducidas por software malintencionado"[50].

Aparte de este pesimista panorama, los expertos coinciden en que el carácter imprevisible de las ciberarmas puede ocasionar daños de magnitud indeterminada, no sólo para las víctimas, sino también para los atacantes. Kemp ejemplifica esta paradoja con los efectos colaterales que produjo la puesta en marcha de un programa de ciberarmas que, bajo el nombre en clave de "The Olympic Games", "fue diseñado para sabotear infraestructuras de otro país"[51], y que fue revelado en un extenso trabajo de investigación publicado en The

[49] Kaspersky Security Bulletin 2012. Desarrollo de las amenazas informáticas en 2012, 5 de diciembre de 2012. Disponible en http://www.viruslist.com/sp/analysis?pubid=207271194#1 . Fecha de la consulta 02.12.2013.
[50] KEMP R. Scott, Cyberweapons: Bold steps in a digital darkness?, 7 de junio de 2012. Disponible en http://www.thebulletin.org/cyberweapons-bold-steps-digital-darkness . Fecha de la consulta 26.11.2013.
[51] Ibid.

New York Times[52].

El proyecto, según cita la investigación, tendría como objetivo los sistemas informáticos iraníes que controlan las principales plantas nucleares. The New York Times sitúa el germen de "The Olympic Games" en 2006, bajo la Administración de George W. Bush, en un momento en que las relaciones estadounidenses con Irán atravesaban un momento delicado, después de que el gobierno de Teherán retomara el enriquecimiento de uranio en la planta subterránea de Natanz. Las susceptibilidades fueron en aumento cuando el presidente iraní Mahmoud Ahmadinejad hizo pública su intención de que la planta acogiera más de 50.000 centrifugadoras.

La investigación publicada justifica la presencia de Israel en el proyecto por dos motivos estratégicos: por una parte, poseían información importante para garantizar el éxito de la operación y, por otra, y de especial interés para los Estados Unidos, esta participación les disuadía de lanzar un ataque militar preventivo contra las instalaciones iraníes.

"En cierto modo, la visión estratégica de "The Olympic Games" es encomiable", afirma Kemp. "Los ciberataques podrían reducir la presión israelí para realizar ataques militares convencionales, que podrían haber conducido a una guerra con Irán, y haber activado la carrera armamentística iraní. Además, esta ciberestrategia también habría dado más oportunidades a la diplomacia"[53]. Pero algo salió mal.

En 2010, salió a la luz pública y de una manera totalmente accidental, Stuxnet, el primero de los elementos del proyecto. Un fallo de programación permitía que el gusano escapase de los sistemas informáticos de la estación de Natanz y se distribuyera por todo el mundo vía Internet. El virus había dado su primer golpe dos años antes, infectando los ordenadores y logrando destruir 1.000 centrifugadoras de gas, pero tras ser detectado y anulado, la capacidad de reacción de Irán fue inesperada.

Según datos de la International Atomic Energy Agency (IAEA) citados por Kemp, el gobierno de Teherán consiguió aumentar sus reservas de uranio empobrecido a niveles superiores a los registrados antes del ataque[54]. La segunda consecuencia fue la puesta en marcha de un cibercomando iraní que, según anunció el General Gholam-Reza Jalali, defendería a su país

[52] The New York Times, Obama Order Sped Up Wave of Cyberattacks Against Iran, 1 de junio de 2012. Disponible en http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r&_r=1& . Fecha de la consulta 22.11.2013.
[53] Ibíd.
[54] The Telegraph, Stuxnet worm 'increased' Iran's nuclear potential, 15 de mayo de 2013. Disponible en http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html . Fecha de la consulta 11.12.2013.

de los enemigos en la red[55].

CONCLUSIONES

Son muchos los factores que han obligado a los gobiernos a buscar las fórmulas de respuesta más ecuánimes a los ciberataques, siempre ante la incertidumbre de quién será su próximo enemigo en la red, cuáles serán los objetivos perseguidos y si sus vulnerabilidades son conocidas por éste. A falta de una regulación legislativa internacionalmente aceptada que persiga a los autores y penalice los actos delictivos cometidos en el ciberespacio, son dos las posturas que los gobiernos pueden adoptar: invertir en defensa o promocionar los medios de ataque. En opinión de Kemp para las naciones altamente desarrolladas y aquellas que dependan "crítica y profundamente de los ordenadores, el enfoque más seguro es dirigir la investigación en el ciberespacio hacia aplicaciones puramente defensivas".

Las actividades en el ciberespacio han modificado sustancialmente el panorama geopolítico mundial, las alianzas entre países pueden perder parte de su solidez ante la sospecha de que el socio incondicional se convierta, en un momento dado, en el enemigo en la red. El siguiente paso es fundamental: se hace preciso un acuerdo global que articule leyes internacionalmente aceptadas para restringir y controlar el uso de las ciberarmas. Aunque este hecho no permita definir la presencia de un gobierno tras su empleo contra otra nación, sí contribuirá a evitar acciones de represalia inadecuadas.

Como bien concluye Kemp "es evidente que la antigua doctrina de disuasión utilizada durante la guerra Fría no es fácilmente aplicable en el ciberespacio. No se entiende bien en qué consistiría y cómo se podría alcanzar esa disuasión, y lo más importante, el enemigo será casi siempre muy difícil de identificar".

Eguskiñe Lejarza Illaro
Periodista

[55] Iran Politik, General Jalali: "Iran has begun to operate its first cyber army", 21 de febrero de 2012. Disponible en http://www.iranpolitik.com/2012/02/21/news/general-jalali-iran-begun-operate-cyber-army/. Fecha de la consulta 21.11.2013.