ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

03/2015 05 de enero de 2014

*José Luis Aznar Lahoz**

EVOLUCIÓN DE LOS MODELOS DE CONFRONTACIÓN EN EL CIBERESPACIO

EVOLUCIÓN DE LOS MODELOS DE CONFRONTACIÓN EN EL CIBERESPACIO

Resumen:

Desde que John T. Draper, también conocido como Captain Crunch, "hackeara", a principios de la década de los 70, las líneas telefónicas de AT&T mediante un pequeño silbato adaptado[1], hasta los últimos acontecimientos, descubiertos en mayo, relacionados con ataques cibernéticos practicados durante años por el gobierno chino a empresas de Estados Unidos, vinculados con el espionaje industrial, o las escuchas de la NSA a la canciller Angela Merkel, han pasado muchos años. Los ataques cibernéticos han superado una diversidad de estadios, desde los más puramente románticos "por amor al arte", hasta los más sofisticados de la actualidad, que involucran a gobiernos atacando a otros gobiernos u organizaciones internacionales como OTAN. La magnitud alcanzada, ha obligado a estos a emplear medios proporcionales a los ataques a los que se enfrentan, creando policías especializadas en el tema e incluso ejércitos preparados para combatirlos y empleando a los servicios de inteligencia de los países, en la defensa de los mismos. A día de hoy, únicamente defensa, pero ya se comienza a especular con la posibilidad de ataques. Esta escalada de actividad cibernética crea un marco de desarrollo en el que se vislumbra un futuro espectacular de ataque-defensa en los próximos años. Hasta dónde puede llegar sólo es fruto de la especulación y de la más ¿singular imaginación?.

Abstract:

It has been a long time, since John T. Draper, also known as Captain Crunch, broke into AT&T landlines in the early 70s by means of a handcrafted whistle[1], until the last events, discovered in May, related to cyberattacks and developed for years by the Chinese government to U.S. companies, linked to industrial espionage, or the NSA listening to Chancellor Angela Merkel's cellphone. Cyberattacks have overcome a variety of stages, from purely romantic reasons, to the recent ones with a level of sophistication and technical complexity, involving governments attacking other governments or

[1] ROSENBAUM, R., "Secrets of the Little Blue Box" *Esquire,* pp. 117 - 125 & 222 - 226, October 1971.

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

international organizations, e.g. NATO. The high number and magnitude of those attacks made the organizations under attack to react in a proportional way in order to gain control and minimize the effects, creating specialized police forces, or even specialized squads in the military and the intelligence agencies. The latest trend in cyber defense not only involving counter-measures to defend and react against an attack, but also active warlike actions in order to gain initiative and control in the network. This rise in the cyber activity creates a perfect enviroment for attack and defense development frameworks with a promising future in the short and medium term. The final evolution of this scene could be only limited by speculation. And maybe, pure imagination?.

Palabras clave:

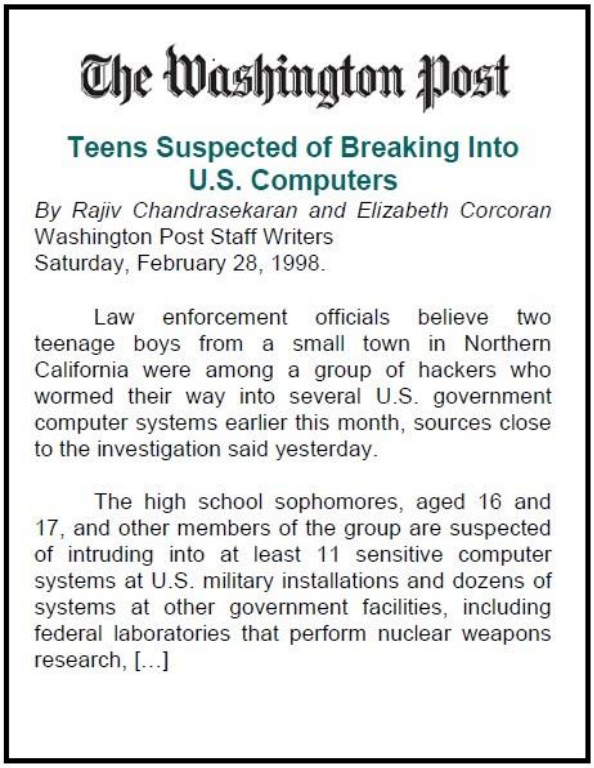
Ciberespacio, ciberguerra, ciberdefensa, ciberguerrero, hacker, DDOS, APT, Stuxnet, ataque cibernético, Mando de ciberdefensa, infraestructura critica.

Keywords:

Cyberspace, cyberwarfare, cyber defense, cyberwarrior, hacker, DDOS, APT, Stuxnet, Cyberattack, Cyber Command, critical infrastructure.

INTRODUCCIÓN

Durante muchos años, noticias como esta (figura 1) inundaban las primeras páginas de la prensa escrita en todo el mundo occidental. Miles de estudiantes y aficionados a la informática probaban sus habilidades para poder romper las barreras que los sistemas ofrecían con el fin de impedir, evidentemente, que personal no autorizado accediera a ellos. A menudo no buscaban otro objetivo que el de demostrar su pericia y la ineficiente capacidad del adversario en administrar y securizar los sistemas, fueran del tipo que fueran.



The Washington Post

Teens Suspected of Breaking Into U.S. Computers

By Rajiv Chandrasekaran and Elizabeth Corcoran
Washington Post Staff Writers
Saturday, February 28, 1998.

Law enforcement officials believe two teenage boys from a small town in Northern California were among a group of hackers who wormed their way into several U.S. government computer systems earlier this month, sources close to the investigation said yesterday.

The high school sophomores, aged 16 and 17, and other members of the group are suspected of intruding into at least 11 sensitive computer systems at U.S. military installations and dozens of systems at other government facilities, including federal laboratories that perform nuclear weapons research, [...]

figura 1. The Washington Post

Evidentemente, los más diestros tenían especial predilección por sistemas como los usados en el Pentágono de los EEUU, la CIA, la bolsa de Nueva York, etc, considerados como los más seguros y mejor protegidos, terminando muchas de las veces por entregarse el saboteador a las autoridades con la finalidad de dar a conocer su hazaña.

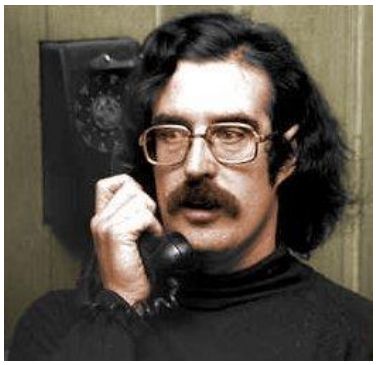
También es cierto que, en numerosas ocasiones, el intruso acababa siendo contratado por el propietario del sistema atacado, ya que, ¿quién mejor puede prevenir el ataque, que aquel que ya ha conseguido atacarlo, conoce sus vulnerabilidades y las "puertas abiertas" por donde entrar al sistema?.

Estos ataques "por amor al arte" han ido evolucionando hasta llegar a otro tipo de ataques y con otras finalidades en la actualidad.

PRIMERAS VIOLACIONES DEL ESPACIO DE COMUNICACIONES

A principios de la década de los 70, John T. Draper (figura 2) modificó un pequeño silbato distribuido como promoción dentro de las cajas de cereales Cap'n Crunch (figura 3), para que emitiera un tono a 2600 Hz. frecuencia que usaba AT&T indicando que la línea

telefónica estaba lista para iniciar una nueva llamada. Mediante esta pequeña operación se entraba en modo operador, siendo posible hacer llamadas gratuitas.



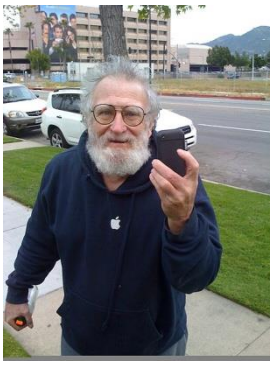


figura 2. John T. Draper.

figura 3. BlueBox

El invento permitió a miles de usuarios de todo el mundo realizar llamadas de larga distancia y conectarse a BBS,s de todo el globo sin coste alguno, con el perjuicio que supuso a las compañías telefónicas. Con esto Draper se ganó el apodo de *Captain Crunch,* con el que es conocido desde entonces, considerándole el primer hacker (phreaker) de la historia de las telecomunicaciones. El sistema telefónico fue modificado de manera tal, que las señales de gestión fueran transmitidas por un sistema separado, impidiendo de esta forma que el fraude continuara.

A mediados de los 70, Draper conoció a dos jóvenes estudiantes de informática interesados en su invento, conocido como *Bluebox*, dedicándose a construirlo y comercializarlo por cincuenta dólares la unidad. Estos dos apasionados de la informática no eran otros sino Steve Jobs y Stephan Gary Wozniak (figura 4), que posteriormente fundaron *Apple Computer.* El dinero recaudado con la comercialización de la Bluebox, permitió, a ambos, financiar el prototipo del primer ordenador Apple: el Apple I.

figura 4. Stephan Gary Wozniak y Steve Jobs

John Draper fue contratado por Apple[2] durante seis meses, antes de que le arrestara el FBI por el fraude cometido. Durante ese tiempo creó un módem para el Apple II, que nunca llegó a comercializarse por su detención en 1977.

En la prisión de Alameda, mientras cumplía su condena, Draper desarrolló una versión de *Forth* con la cual creó *EasyWriter*, el primer procesador de textos que existió para los Apple II.

La historia de John T. Draper, considerado una leyenda en el mundo de la computación y el "hackeo", es un paradigma del universo hacker durante las dos décadas siguientes, en los que se repiten dos circunstancias principalmente:

- La experiencia no se realiza con afán de lucro, sino que la finalidad era la de un mero reconocimiento de habilidades.
- A menudo, el hacker, debido a los conocimientos demostrados, acababa siendo contratado por la empresa atacada u otra del sector.

Aun siendo cierto que John Draper se beneficiaba de realizar llamadas gratuitas por todo el mundo, no puede considerarse esto como un intento de enriquecerse, más aún cuando se daban situaciones tan absurdas como la llamada de larga distancia realizada por Wozniak, simulando ser Henry Kissinger y esperando más de 30 minutos para poder hablar con el Papa, que en esos momentos estaba descansando. De esta forma, en una entrevista publicada por la revista *Esquire* en octubre de 1971, Draper comentó: *"Ya no lo hago, ya no. Y si lo hago, es solo por un motivo, estoy aprendiendo como es el sistema. Hago lo que hago solo para aprender cómo funciona el sistema telefónico"*[3].

Esta situación, aunque se siguió dando, cambió radicalmente hacia finales de los 90 y en la primera década del siglo XXI, años en los que el espíritu de los ataques cibernéticos experimento un vuelco radical.

UN NUEVO ÁMBITO EN LA LUCHA EN EL CIBERESPACIO

Es durante la primera década del siglo XXI, cuando aparecen nuevos paradigmas de ataque a través del ciberespacio. El componente principal que provoca este cambio no es otro que Internet, el auge que experimenta en la vida cotidiana, tanto a nivel individual de cada uno de los usuarios, como a nivel institucional de los gobiernos y también de las corporaciones empresariales.

---

2 «elhacker.net,» elhacker.NET, 16 February 2006. [En línea]. Available: http://www.elhacker.net/hackers-john-draper.html. [Último acceso: 12 August 2014].

3 ROSENBAUM. *Op. cit.*

Cuando ha pasado a ser imprescindible en nuestro quehacer diario es cuando aparecen diversas formas de aprovechamiento de forma fraudulenta. Paulatinamente, desaparece ese componente idealista de los comienzos para convertirse en un acto delictivo, que puede alcanzar enormes dimensiones, ya sea con ánimo de lucro para las personas o como una nueva forma de agresión entre naciones. En estos últimos años varios son los escenarios en los que las naciones han utilizado el ciberespacio para agredir a su enemigo.

Conflicto en Oriente Próximo

Durante miles de años se han sucedido guerras en la zona (figura 5). El 6 de septiembre de 2007, pasada la medianoche, dos aviones israelíes bombardeaban un centro fabril sirio, cerca de la frontera con Turquía, intervención denominada "Operación Huerto" [4]. Ninguno de los dos países dio publicidad a la acción realizada.

figura 5. Zona atacada por Israel al norte de Siria.

A medida que se tuvo conocimiento a nivel internacional del suceso, ambos países justificaron la acción de manera diametralmente opuesta. Siria argumentaba que el centro atacado se encontraba vacío, mientras que Israel afirmaba que en el complejo industrial se fabricaban armas nucleares de diseño norcoreano[5].

[4] FOLLATH, E. & STARK, H., «The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor», 02 November 2009. [En línea]. Available: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html. [Último acceso: 01 November 2014].

[5] KESSLER, G., «N. Korea, Syria May Be at Work on Nuclear Facility», 13 September 2007. [En línea]. Available:

Pero, más allá del hecho que Siria trabajara con armamento nuclear o no, nos centraremos en el suceso en que dos aviones sean capaces de penetrar a través de las defensas antiaéreas de Damasco. Sistemas de defensa de fabricación rusa y de muy alto coste, que en esos momentos Rusia intentaba vender a Irán y cuya venta se vio frustrada.

¿Qué había sucedido en la oscuridad de la noche para que estos aviones, que debían haber iluminado las pantallas de los radares por los que se acercaron, no fueran detectados? ¿cómo fue posible que tecnología rusa del más alto nivel pudiera fallar de este modo, habida cuenta de los intereses comerciales que se estaban barajando en esos momentos?

Tres son las hipótesis que se barajan[6], cada una más espectacular que la anterior, dignas del mejor guion de acción de las factorías de Hollywood:

- **creación de una *puerta trasera*** en el código del programa del sistema de defensa antiaérea ruso, bajo la iniciativa del gobierno de Israel o de alguno de sus aliados, ¿Estados Unidos, por ejemplo?, utilizando a los equipos de desarrolladores que lo implementan, a alguno de sus componentes, capaz de traicionarlo, ya sea por dinero o por convencimiento político.
- **interceptación de la red siria de comunicaciones**, lo que conlleva el descubrimiento de su recorrido y la manipulación del mismo. Teniendo en cuenta que la mayor parte de la misma está constituida por cable de fibra óptica enterrado bajo el desierto, resulta difícil creer que los servicios de inteligencia sirios no sospecharan de la manipulación de la que podían estar siendo víctimas sus infraestructuras de comunicaciones.
- un radar es un equipo de transmisión/recepción de señales electromagnéticas. Un *unmanned aerial vehicle* (UAV), debidamente equipado, podría capturar la señal con la que el radar le ilumina y **devolver, dentro de la señal de retorno, código malicioso** transmitido en la misma frecuencia de la señal radar (figura 6). De esta forma el código se introduciría en los sistemas de defensa antiaérea utilizados por Siria.

http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091202430.html. [Último acceso: 01 November 2014].

[6] CLARKE, R. &KNAKE, R., *Cyber War. The next threat to National Security and what to do about it*, New York: ECCO Press, 2011.

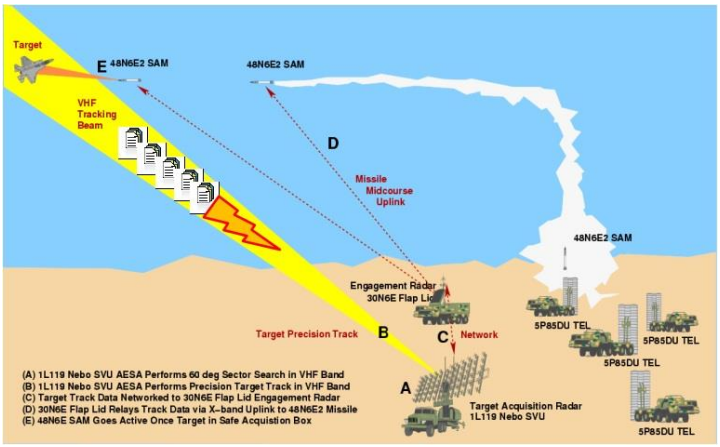


figura 6. Transmisión de código malicioso
a un radar antiaéreo.

Con independencia de cuál fuera la opción elegida, realizaremos una pequeña reflexión acerca de la citada en tercer lugar. Para securizar nuestras redes, las de mando y control incluidas, se proponen siempre una serie de medidas estándar como pueden ser la identificación y autenticación, inhabilitación de elementos extraíbles, el cifrado de mensajes, uso de firewalls, VPN,s[7], instalación de IDS e IPS[8] y otras no mencionadas para no ser exhaustivos, pudiendo llegar hasta el aislamiento absoluto de la red. Pero, ¿qué puede ocurrir cuando el mensaje infectado proviene de un usuario autorizado, desde un equipo reconocido como propio de nuestra red?, ¿cuándo los paquetes que circulan por la red no son más que los datos de navegación de un avión, transmitidos por nuestro radar de vigilancia y que han sido modificados convenientemente (figura 6) para infectar el sistema? ¿Serían nuestros equipos y medidas de seguridad capaces de detener la intrusión? La respuesta es, evidentemente, negativa en una medida mayor del 95%, dejando un pequeño margen de cortesía a la bondad y capacidad de los medios utilizados.

Cualquiera de estas tres técnicas, habría permitido a Israel, apoderarse de los sistemas de defensa antiaérea de Siria y de esta forma "ignorar" la incursión de los dos aviones, obligando a que las armas antiaéreas permanecieran calladas mientras los aviones israelíes dejaban caer plácidamente su carga mortal, en forma de bombas, sobre las instalaciones sirias, sin la preocupación de poder ser abatidos por algún misil antiaéreo.

La utilización del ciberespacio en este caso es la de acompañamiento a las operaciones militares convencionales, leitmotiv, en la última década, cuando las naciones se enfrentan en conflictos armados entre ellas.

7 Virtual Private Network (VPN).
8 Intrusion Detection System (IDS), Intrusion Protection System (IPS).

Ciberataque ruso a Estonia

Este ataque es considerado como uno de los símbolos de la utilización del ciberespacio para el desarrollo de conflictos entre naciones.

figura 7. Estonia.

Estonia (figura 7) se constituía como una de las muchas republicas que componían la extinta URSS. Rusia había erigido por toda Europa del Este enormes estatuas, en recuerdo de sus soldados caídos en la Segunda Guerra Mundial. Las relaciones de las repúblicas satélites con Rusia no eran, precisamente, de amistad y fraternidad. Y Estonia no era una excepción. Durante años se quisieron eliminar los símbolos rusos de ocupación y cuando en 2007 se aprobó la ley que lo ordenaba, miles de estonios salieron a la calle. Entre otros símbolos se derribó la enorme estatua de bronce, que adornaba el centro de Tallinn (figura 8).

figura 8. Revueltas por el derribo de la estatua del soldado ruso en Tallinn, Estonia.

Moscú protestó por lo que de menosprecio a sus muertos significaba tal acción, incrementando, aún más si cabe, la tensión entre ambos pueblos.

Estonia es un país altamente dependiente de las Tecnologías de la Información y la Comunicación, comparable a Corea del Sur, constituyendo, ambas, las sociedades más vinculadas al ciberespacio del planeta. El mismo día que ocurrieron estos hechos, servidores web estonios recibieron millones de solicitudes que no fueron capaces de responder y se colapsaron. Los servicios web fueron inaccesibles para la población, no pudiendo utilizar los servicios de banca online y los gubernamentales, principalmente.

Se estaba produciendo un ataque DDOS, que colapsó a la sociedad estonia, obligando a desconectar las "fronteras cibernéticas" del país. Miles de ordenadores enviaban solicitudes a servidores concretos, impidiendo el acceso a los mismos. El ataque se realizaba mediante una red de "zombis" que constituían una botnet. Los ordenadores habían sido "robados" sin que sus propietarios se hubieran percatado. Durante la realización de los ataques el usuario no era consciente del mismo, dado que podía seguir utilizándolo, apreciando, a lo sumo, una pequeña disminución en el rendimiento, fácilmente achacable a una congestión puntual de las aplicaciones y a la conexión a la red del ordenador.

Sitios web de organismos gubernamentales, bancos, empresas o periódicos quedaban inaccesibles durante días dejando paralizado al país. El Hansapank, uno de sus bancos más importantes sufrió grandes pérdidas. Muchos de los servicios telefónicos dejaron de funcionar. Todo esto se prolongó durante algunas semanas, lo que, supuestamente, llevo a Estonia a solicitar el auxilio de OTAN, invocando el Artículo 5 del Tratado, por el cual, en caso de un ataque armado contra uno de sus miembros, el resto de naciones debería acudir en su auxilio. Aunque posteriormente Andrus Ansip, primer ministro estonio, desmintiera este hecho[9], de haber fructificado tal solicitud, el conflicto hubiera alcanzado dimensiones internacionales, difícilmente imaginables. Se ha llegado a denominar este caso como la primera guerra en la web, *Web War I (WWI),* aprovechando la coincidencia de siglas con las de la primera guerra mundial, *World War I (WWI).*

Para intentar resolver el problema, se rastrearon las direcciones de los ordenadores zombis, perdiéndose la pista en Rusia. Esto provocó que Estonia la acusara de ser la causante del ataque, lo que, sin ningún lugar a dudas, negó. Achacó los hechos a patriotas rusos que, por iniciativa propia, respondieron a la ignominia sufrida.

El resultado final fue la creación de un Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (Cooperative Cyber Defence Centre of Excellence, CCDCOE) con misiones de investigación y formación en el marco del ciberespacio[10]. Lo que hizo singular

[9] HERNANDEZ, A., «TICbeat,» 28 March 2014. [En línea]. Available: http://seguridad.ticbeat.com/de-estonia-ucrania-la-evolucion-de-los-conflictos-en-el-ciberespacio/. [Último acceso: 09 August 2014].

[10] «CCDCOE NATO Cooperative Cyber Defence,» [En línea]. Available: https://www.ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html. [Último acceso: 10 August 2014].

esta confrontación entre naciones fue el hecho, totalmente contrario al caso anterior, de no utilizar la fuerza armada como complemento a las acciones en el ciberespacio, amén de la magnitud de los resultados alcanzados.

Enfrentamiento entre Georgia y Rusia

Otra vez, Rusia vuelve a ser protagonista de una nueva acción en el ciberespacio. En esta ocasión el detonante del conflicto no fue otro que la disputa por la soberanía de dos provincias limítrofes (figura 9) a Rusia y a Georgia: Osetia del Sur y Abjasia.

figura 9. Frontera entre Rusia y Georgia.
Osetia del Sur y Abjasia.

Como ya se ha comentado, las relaciones entre Rusia y la mayoría de las repúblicas de la extinta URSS nunca se han caracterizado por su grado de buena concordia.

En 1991, Georgia se declara república independiente, constituyendo un gobierno propio con Mijail Saakachvili al frente como presidente. Al año siguiente, las provincias de Osetia del Sur y Abjasia se proclaman independientes, expulsando a los ciudadanos georgianos de su territorio por la fuerza, contando con el apoyo del Kremlin.

Años más tarde, en agosto de 2008, cuando fuerzas de Osetia del Sur atacaron territorio georgiano, el ejército de este país respondió mediante un ataque de fuerza. Frente a este ataque, el ejército ruso respondió expulsando al ejército georgiano de Osetia del Sur.

Al mismo tiempo, Rusia lanzo un ataque cibernético contra las páginas web de los medios de comunicación y el gobierno de Georgia[11]. Diferentes servidores web sufrieron un

[11] GANUZA, N., «La Situación de la Ciberseguridad en el Ambito Internacional y en la OTAN» de *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, Madrid, Instituto Español de Estudios Estrategicos, 2011, pp. 167 - 214.

ataque DDOS, al mismo tiempo que se bloqueó el acceso desde Georgia a los servicios de la CNN y la BBC.

Georgia se conecta a Internet a través de Rusia y Turquía. Los routers se vieron colapsados, incapaces de dirigir el tráfico hacia el exterior del país. El gobierno se vio forzado a localizar sus páginas web fuera del territorio, en servidores de Google localizados en California. Para defenderse de los ataques provenientes de Rusia, Georgia intentó bloquear el tráfico que provenía de su vecino, a lo que los rusos respondieron redirigiendo los ataques para que se materializaran desde China.

El sector bancario georgiano también se vio afectado, por lo que, ante la posibilidad de que se produjera un robo masivo de información, decidieron bloquear las operaciones online. Los ciberguerreros rusos, cuando se vieron incapaces de acceder a los servidores, variaron la estrategia. Dirigieron el ataque contra la banca internacional, simulando que se estaba produciendo desde Georgia. La respuesta fue inmediata, cortando la mayor parte de los bancos extranjeros las operaciones con los bancos georgianos.

El conflicto, que como se ha expuesto, alcanzó dimensiones internacionales, obligó a intervenir a la comunidad internacional, representada por el presidente francés Nicolás Sarkozy[12]. Este llegó a conseguir un acuerdo por el que Rusia se comprometía a abandonar Georgia. Es en estos años cuando se gesta la compra de buques de asalto anfibio por parte de la Armada Rusa. En diciembre de 2010 se anuncia, por el presidente Sarkozy, la firma del contrato para la adquisición de dos buques (más dos opcionales) de la clase Mistral, siendo rubricado por el Viceprimer Ministro ruso Igor Sechin y el Ministro de defensa francés Alain Juppé, el 25 de enero de 2011. ¿Podría ser esta una de las consecuencias de las actividades en el ciberespacio?. Si esto es cierto, nunca se sabrá, como ocurre habitualmente en estas circunstancias.

Regresando al conflicto entre Georgia y Rusia, una vez más, esta última negó la autoría de las acciones realizadas en el ciberespacio, aunque por experiencia se sabe que cuando se realizan actividades a gran escala desde territorio ruso, los servicios de inteligencia del estado están a la sombra de los acontecimientos. La comunidad internacional está plenamente convencida de que en el desarrollo de estas actividades Rusia no ha desplegado todo su potencial, dejando sus mejores ciberarmas para cuando verdaderamente las necesite.

Nuevamente, un ataque en el ciberespacio se realiza como acompañamiento de un enfrentamiento convencional entre sociedades confrontadas. Los principales ejes sobre los que se desarrollan los acontecimientos cibernéticos se encuentran en los entornos

[12] McGUINNESS, D., «BBC News Europe,» 08 October 2011. [En línea]. Available: http://www.bbc.co.uk/news/world-europe-15206738. [Último acceso: 12 August 2014].

económicos y de la información, con agresiones a los sistemas bancarios y limitación al acceso a la información.

Otra característica repetida es la ausencia de pruebas que hagan posible inculpar de la autoría de los hechos[13], permitiendo al presunto culpable, negarlos. Al hilo de estos sucesos, es posible, también, redireccionar los ataques, de tal forma que terceros resulten sospechosos de su ejecución.

Hostilidades entre la dos Coreas

Durante la primera mitad de 2009 un nuevo conflicto se estaba incubando en el escenario internacional. ¿Nuevo?. No sería correcto calificar la hostilidad entre Corea del Norte y Corea del Sur (figura 10) como nueva. Así, en mayo de ese año, Corea del Norte explosionó una bomba nuclear como parte de sus experimentos nucleares. Se trataba, además, de una forma de someter a una presión mayor a las sociedades occidentales.

figura 10. Corea del Norte y Corea del Sur.

Estados Unidos programó un ejercicio de ciberguerra en la zona, denominado "Cyber Storm"[14], al que se unieron Japón y Corea del Sur. Se desconoce si se realizó como represalia a los experimentos nucleares de Corea del Norte, pero esta lo asumió como una maniobra de distracción para la invasión de su territorio.

[13] TORRES, M., «Los dilemas estratégicos de la ciberguerra» *Revista Ejército,* nº 839, pp. 14 - 19, 2011.
[14] CLARKE. *Op. cit.*

En venganza, Corea del Norte respondió con el lanzamiento de misiles y un ataque dentro del ciberespacio. Este consistió en un DDOS mediante la utilización de botnets, dejando sin servicio a diferentes webs gubernamentales de los Estados Unidos. Entre otros se vieron afectados el Departamento del Tesoro, los Servicios de Inteligencia, la Bolsa de Nueva York y la bolsa de valores NASDAQ. También las webs del *Washington Post* se vieron bloqueadas[15].

Se intentó dirigir el ataque DDOS, también, contra la Casa Blanca. Esta había sido atacada unos diez años antes y se habían tomado las medidas oportunas[16]. Estas consistían en que los servicios web de la Casa Blanca estaban ubicados en una *Content Delivery Network,* CDN, por lo que cualquier petición era redirigida hacia el servidor más cercano. Así, el ataque fue, en efecto, redirigido hacia el servidor más cercano, con lo que los servicios de la Casa Blanca en el Suroeste asiático estuvieron bloqueados durante algún tiempo, pero no en el resto del mundo.

Igualmente los servidores surcoreanos fueron atacados. Evidentemente se sospechó de Corea del Norte, pero esta negó la autoría de las acciones realizadas.

Corea del Norte dispone de Unidades militares dedicadas a la realización de ataques en el ciberespacio. Sus ciberguerreros son reclutados desde la escuela primaria, donde son elegidos de entre los mejores para convertirlos en auténticos especialistas en acciones de ciberguerra.

Estados Unidos determinó que la verdadera finalidad de los ataques de Corea del Norte estaban orientados a obtener información de las capacidades de las infraestructuras de telecomunicaciones de Corea del Sur para soportar un ataque DDOS, ya que en caso necesario, serían estas comunicaciones las que utilizaría Estados Unidos ante un conflicto en la zona, además de localizar la situación de armas de destrucción masiva en posesión de Corea del Sur.

Nuevamente, el ataque cibernético tiene lugar junto a acciones de otro tipo. En este caso no se trata de conflicto armado, sino, más bien, de una tentativa de amenaza, indicando al enemigo las capacidades que sería capaz de desarrollar si el conflicto fuera real. De igual forma, tampoco se reconocen los hechos realizados en el ciberespacio, dado que es muy difícil demostrar su autoría, gracias a la capacidad de realizar el ataque desde posiciones que no son las propias.

---

15 «ccn-cert.cni.es,» Centro Criptológico Nacional, 09 July 2009. [En línea]. Available: https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2218:ataque-ddos-a-gran-escala-afecta-a-eeuu-y-corea-del-sur&catid=61&Itemid=197&lang=es. [Último acceso: 15 August 2014].

16 LEMOS, R., «Hackers cripple White House site» 04 May 2001. [En línea]. Available: http://news.cnet.com/Hackers-cripple-White-House-site/2100-1001_3-257068.html. [Último acceso: 15 August 2014].

De los casos presentados hasta el momento, este es el primero en el que el adversario más débil es el que realiza el ciberataque. Esto resulta sorprendente, dado que gracias a la facilidad de realización y el bajo coste de ejecución son condiciones que facilitan que este fuera el caso más habitual.

figura 11. Guerrero convencional y ciberguerrero.

De hecho, la ciberguerra es una forma de guerra asimétrica. No es necesario un sofisticado armamento, ni grandes ejércitos para desarrollarla. Solo es necesario un ordenador y los conocimientos informáticos suficientes (figura 11) para llevarla a cabo, pudiéndose realizar desde cualquier lugar del mundo, incluso, más normal, desde varios simultáneamente, siendo difícil la identificación del atacante y, por ende, mas fácil el mantenimiento del anonimato del mismo, pudiendo ser sus efectos iguales, o incluso más, devastadores que los de una guerra convencional[17].

LA GUERRA LLEVADA MÁS ALLÁ DEL CIBERESPACIO

Hasta este momento hemos estudiado diversos casos que han tenido lugar en los últimos años, pero que su escenario se encontraba en los sistemas de comunicaciones y la forma de aprovecharse de ellos o impedir que el enemigo pueda utilizarlos, al menos que no pueda realizarlo de una forma fácil y cómoda.

Pero, debido a la proliferación que el microprocesador ha tenido en el devenir de la vida cotidiana, en el amplio espectro de sistemas actuales que lo incorporan para su habitual

[17] SANCHEZ, G.,«Internet: Una Herramienta para las Guerras en el Siglo XXI»*Politica y Estrategia,*nº 114, pp. 21 - 31, 2009.

funcionamiento ayudado por un software que gestione su labor, se ha creado una nueva situación. Estos sistemas pueden ser desde una sencilla lavadora hasta el más sofisticado satélite de comunicaciones situado en el espacio. Aquellos sistemas cuya finalidad es la de controlar y supervisar procesos industriales a distancia constituyen lo que se ha denominado sistemas SCADA (figura 12), Supervisory Control And Data Acquisition.

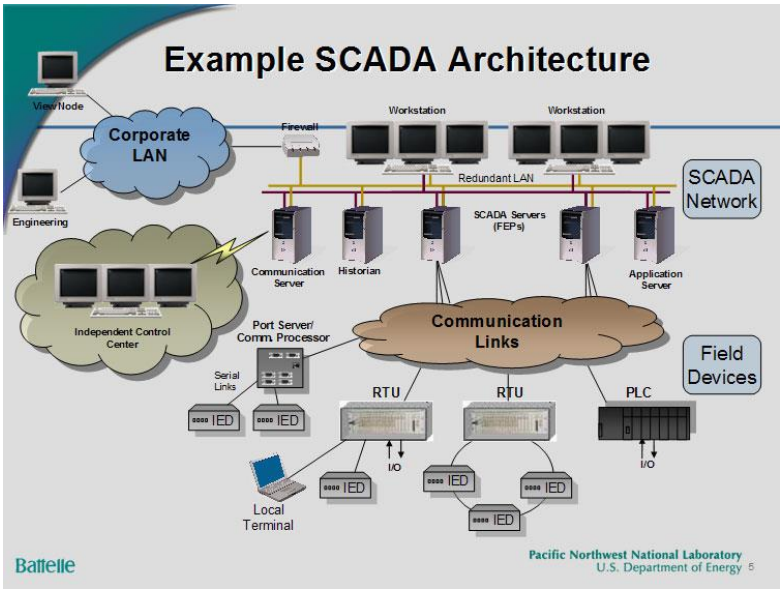


figura 12. Arquitectura de sistemas SCADA.

Es a estos sistemas a los que los nuevos ciberguerreros han comenzado a atacar. No es necesario afirmar que las técnicas que hay que utilizar no son las mismas que en los casos anteriores, pero sí que, de las técnicas utilizadas para aquellos, se han extraído enseñanzas para estos.

El caso mundialmente conocido es el del virus Stuxnet[18], un tipo de troyano muy sofisticado que utiliza accesos privilegiados de root (rootkit). El virus se instala en el sistema operativo del sistema y se queda "esperando" hasta el momento de su activación. Este tipo de ataque se conoce como *Advanced Persistent Threat*, APT, y Stuxnet tiene la consideración de ser uno de los mayores ejemplos de la historia.

[18] JOYANES, L., «Estado del Arte de la Ciberseguridad» de *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, Madrid, Instituto Español de Estudios Estrategicos, 2011, pp. 13 - 46.

La forma de transmisión del Stuxnet, dado que los sistemas de control de una central nuclear no están conectados con el exterior, fue mediante la utilización de una memoria USB con el virus instalado y listo para propagarse en el momento que la memoria se conecta a un ordenador del sistema de mando y control. Stuxnet fue detectado por primera vez en junio de 2010 por Sergey Ulasen, joven investigador y desarrollador de software en una pequeña compañía de seguridad informática de Bielorrusia, VirusBlokAda, que lo descubrió en un ordenador de un cliente de Irán[19]. Como ocurre tradicionalmente en estos casos, en agosto de 2011, Sergey Ulasen pasó a formar parte de la nómina de empleados de Kaspersky Lab, multinacional especializada en seguridad informática, ampliamente reconocida.

Fue precisamente para atacar a Irán para lo que se diseñó el virus. A lo largo de la segunda mitad del siglo pasado, Irán, como uno de los países más influyentes de Oriente Próximo, siempre ha deseado construir su propio armamento nuclear. Inicialmente contó con el apoyo de los países occidentales, principalmente de Estados Unidos, pero cuando el país se tornó radical islámico, sus aliados intentaron frenarlo por todos los medios.

Con la llegada del nuevo siglo, el programa nuclear iraní se encontraba muy avanzado, de tal forma que los servicios de inteligencia norteamericanos anunciaron que Irán tendría capacidad armamentística nuclear en 2012. Esto suponía un grave peligro en la zona. No debemos olvidar que el país comparte vecindad con Israel, eternos enemigos y principal aliado de Estados Unidos.

Se intentó detener por todos los medios el avance del citado programa, mediante todo tipo de acciones, como el embargo de importaciones de petróleo provenientes de Irán, pasando por sanciones al Banco Central de Irán y hasta el bloqueo del estrecho de Ormuz, de gran importancia estratégica debido a que se encuentra en la salida del golfo Pérsico, siendo pieza clave para el control del petróleo, ya que aproximadamente el 40% de la producción petrolífera mundial se exporta a través de él.

A pesar de todo, Irán siguió avanzando en su programa nuclear, por lo que se hizo necesario algún otro tipo de medidas que, al menos, lograran retrasarlo.

[19] KASPERSKY, E., «Nota Bene: Eugene Kaspersky´s Official Blog,» 2 November 2011. [En línea]. Available: http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/. [Último acceso: 17 August 2014].

figura 13. Centrifugadoras de uranio de las centrales nucleares iraníes.

En esos momentos apareció Stuxnet, un programa dañino diseñado para interceptar ordenes enviadas en un sistema SCADA, y así controlar las funciones dentro de instalaciones industriales. El ataque de este virus se centraba sobre los variadores de frecuencias que controlaban la velocidad de los motores de rotación de las centrifugadoras de uranio (figura 13), proceso necesario para su enriquecimiento. Además, se ha comprobado que Stuxnet no afecta a cualquier variador de frecuencia.

La complejidad de Stuxnet es inusual. El programa comprueba los sistemas de la instalación industrial atacada, afectando únicamente a los controladores lógicos programables (PLC) fabricados por Siemens. El ataque requiere conocimientos de procesos industriales. El virus solo se activa si encuentra 33 variadores fabricados por las empresas Vacon de Finlandia o Fararo Paya de Irán, que son los utilizados por las plantas de enriquecimiento iraníes, estableciéndose rutinas distintas según la cantidad de variadores de uno y otro fabricante[20]. De esta forma se "aseguraba" que era iraní y que tenía cierta entidad. Aun así, otras plantas repartidas por todo el mundo que utilizaban los mismos controladores se vieron afectadas. El resultado final era la destrucción de las centrifugadoras.

Stuxnet aprovecha vulnerabilidades de día cero del sistema operativo Windows[21]. Este tipo de vulnerabilidades tienen gran probabilidad de éxito, cada una de ellas por separado, aunque estén instaladas todas las actualizaciones, al no ser conocidas públicamente. No es habitual atacar un mismo sistema con más de una de estas vulnerabilidades ya que supone hacerlas públicas.

[20] FALLIERE, N. et al, W32.Stuxnet Dossier, Cupertino, USA: Symantec Corporation, February 2011.
[21] KASPERSKY. *Op. cit.*

Otras características conocidas de esta APT son su elevado tamaño y su sofisticada arquitectura, en la que se emplearon técnicas de ingeniería del software, realizándose un desarrollo modular por diversos equipos trabajando en paralelo. Stuxnet está firmado digitalmente con dos certificados auténticos robados de autoridades de certificación[21].

Este intrincado escenario, digno de una de las mejores obras de John le Carré, ambientadas en la guerra fría, inclina la balanza de las sospechas sobre la autoría del ataque hacia Estados Unidos e Israel, en conjunta colaboración, para eliminar a Irán como potencial enemigo nuclear en la zona. Al igual que cuando de ataques a sistemas de telecomunicaciones se trata, ninguno de estos países reconoció la autoría del Stuxnet. Se supone que, además de los hechos relatados, el virus se encargó de recopilar información de las plantas nucleares y enviarla hacia el exterior, camino de vuelta a los servicios de inteligencia de ambas naciones.

¿QUÉ ESTA OCURRIENDO HOY EN EL CIBERESPACIO?.

La actividad cibernética tiene lugar, hoy en día, en cualquier instante. Con total seguridad, mientras leemos estas líneas, están teniendo lugar acontecimientos en el ciberespacio que comprometen nuestra forma de vida en mayor o menor grado.

En el mes de mayo, esta noticia (figura 14) saltaba a todos los diarios del mundo. Cinco oficiales chinos, como consecuencia de las imputaciones de un informe publicado por la compañía de ciberseguridad MANDIANT, eran acusados por el Departamento de Justicia de Estados Unidos de espionaje industrial a Westinghouse Electric, the United States Steel

Corporation, Alcoa Inc, Allegheny Technologies, SolarWorld y otras empresas multinacionales americanas, proporcionando ventajas comerciales a competidores chinos.

El FBI y agencias de inteligencia estadounidenses como la CIA o la NSA fueron capaces de rastrear el ataque, determinando que fue realizado por miembros del "Tercer Departamento" del Ejército de Liberación Popular, considerado como la NSA china, operando desde la sede (figura 15) de la "unidad 61398" en Shanghái. Un edificio militar de 12 plantas en Datong Road, fuertemente custodiado, cerca del aeropuerto. La unidad 61398, está compuesta por personal entrenado en el desarrollo de capacidades de seguridad informática (¡preferentemente en quebrantarlas!). Durante años han sido siempre acusados de ser la fuente de ataques informáticos chinos. Se sospecha que España también ha sido "ciberatacada" por esta Unidad militar del Ejército chino.

The New York Times

5 in China Army Face U.S. Charges of Cyberattacks

By MICHAEL S. SCHMIDT and DAVID E. SANGER
May 19, 2014

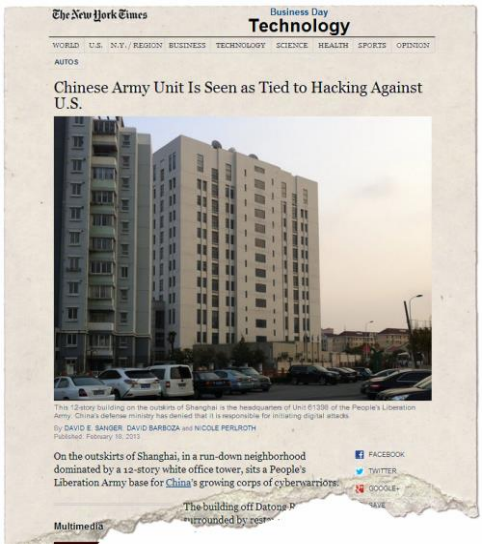
WASHINGTON — In the Obama administration's most direct confrontation with China over its theft of corporate secrets, the Justice Department on Monday unsealed an indictment of five members of the Chinese People's Liberation Army and charged them with hacking into the networks of Westinghouse Electric, the United States Steel Corporation and other companies.

The indictment named members of Unit 61398, which was publicly identified last year as the Shanghai-based cyberunit of the People's Liberation Army, including its best-known hackers known online by the noms de guerre "UglyGorilla" and "KandyGoo."

The F.B.I. and American intelligence agencies electronically tracked the activities of the hackers, one official said, and "put them inside the Datong Road headquarters" of the cyberunit, a heavily guarded 12-floor military tower near the Shanghai airport.

[...]

figura 14. The New York Times



The New York Times — Business Day — Technology

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION AUTOS

Chinese Army Unit Is Seen as Tied to Hacking Against U.S.

On the outskirts of Shanghai, in a run-down neighborhood dominated by a 12-story white office tower, sits a People's Liberation Army base for China's growing corps of cyberwarriors.

Multimedia

figura 15. Sede de la Unidad 61398 en Shanghái

Era el mes de junio del pasado año, cuando un escándalo, que alcanzó inusitadas proporciones, copaba la primera plana de todos los noticiarios mundiales. Un joven administrador de sistemas, subcontratado por el gobierno de los Estados Unidos a través de Booz Allen Hamilton Inc., uno de los mayores contratistas en asuntos militares y de inteligencia, filtraba a los medios miles de documentos clasificados de alto secreto. Los informes filtrados a la prensa por Edward Snowden desvelaban el complejo entramado de agencias de inteligencia de numerosos países occidentales, capitaneadas por la National Security Agency (NSA) de Estados Unidos, mediante el cual se establecía un sistema de vigilancia globalizada, recopilando datos, registros, documentos y comunicaciones de todo tipo, utilizando programas secretos de

vigilancia masiva como PRISM o XKeyscore y rompiendo la seguridad de los sistemas operativos iOS, Android, o la violación de los cifrados de las BlackBerry. Tan globalizado

resultó ser que Estados Unidos estaba vigilando a sus propios aliados. El caso que más repercusión mediática obtuvo fue el de las escuchas de conversaciones telefónicas a la canciller alemana Angela Merkel, creando un conflicto diplomático entre los dos mandatarios, Merkel y Barack Obama (figura 16), y entre los dos países, pidiendo Alemania explicaciones de los hechos a Estados Unidos. Aunque, en principio, no se encuentra directamente relacionado con el ciberespacio, cabe destacar que se siguen produciendo hechos similares, cuya consecuencia más conocida es la reciente expulsión del país del jefe de la CIA en Berlín, según informó Clemens Binninger, presidente de la comisión parlamentaria que supervisa los servicios secretos alemanes.

figura 16. Angela Merkel y Barack Obama

Tales dimensiones alcanzó el escándalo que se destaparon todo tipo de prácticas fraudulentas de las agencias de inteligencia occidentales, principalmente de la NSA, como capturar y almacenar datos privados de cualquier individuo a lo largo y ancho de todo el mundo, creando perfiles con los que deducir su modo de vida[22]. También se almacenaron millones de transacciones financieras. Todas las informaciones apuntaron a que las mayores empresas de telecomunicaciones y del sector colaboraron de una forma "más o menos voluntaria" mediante la cesión masiva de datos de sus clientes, además del acceso a sus servidores. Entre estas empresas se encuentran: Microsoft, Google, Apple, Facebook y otras más.

Por último, como uno de los casos más recientes y de mayor repercusión mundial alcanzada, citaremos el "¿enfrentamiento entre las dos Coreas?", que tuvo lugar en el mes de marzo del pasado año. Corea del Sur recibió ataques cibernéticos que pudieron paralizar servidores de seis de sus principales bancos, impidiendo a sus clientes realizar operaciones de banca electrónica y la utilización de sus cajeros automáticos. Rastreada la dirección de dónde provenía el ataque, se llegó hasta China, donde, como era previsible, se pierde su rastro.

Tratándose de Corea del Sur, se sospecha, como no puede ser de otra forma, que Corea del Norte pudo estar implicada, no teniéndose, hasta el momento, evidencias de que este punto pueda ser cierto.

---

[22] GREEWALD, G., «theguardian,» 31 July 2013. [En línea]. Available: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. [Último acceso: 20 August 2014].

El ataque no "afectó" al gobierno surcoreano, a sus fuerzas armadas o a su inteligencia, …y si lo ha hecho, nunca lo sabremos, porque como se ha repetido en numerosas ocasiones, los acontecimientos que se producen en el ciberespacio no se reconocen, …por ninguno de ambos bandos.

figura17. Almirante Michael S. Rogers
Director NSA

Todo lo anterior ha llevado a las naciones a ejercer su derecho a defenderse por tierra, mar y aire y, en estos momentos, también en el ciberespacio. Uno de los primeros países, sino el primero, es como siempre Estados Unidos, creando en junio de 2009 el **Cyber Command** (USCYBERCOM), nombrando comandante en jefe al General Keith B. Alexander, siendo a su vez el Director de la National Security Agency, NSA, agencia de inteligencia encargada de todo lo relacionado con la seguridad de la información, como parte del Departamento de Defensa. Recientemente, en el mes de marzo, el Presidente Obama ha nombrado al Almirante Michael S. Rogers (figura 17) nuevo Director de la NSA, en sustitución del General Alexander.

«El USCYBERCOM planea, coordina, integra, sincroniza y conduce actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los Estados Unidos y sus aliados en el ciberespacio e impedir lo mismo a nuestros adversarios»[23].

[23] «Wikipedia, The Free Encyclopedia,» Wikimedia project, 17 April 2013 . [En línea]. Available:

En España, se están llevando a cabo diversas políticas de defensa contra este tipo de acciones delictivas. Se han creado diversos organismos con competencias relacionadas, como las unidades especializadas en delitos telemáticos de la Policía Nacional y de la Guardia Civil. Los servicios de inteligencia nacionales, CNI, también han realizado acciones sobre este tema.

figura 18. General López de Medina Comandante Jefe del MCCD.

En los últimos años se ha pretendido unificar criterios en esta materia mediante la confección del Esquema Nacional de Seguridad, pilotado por el CCN-CERT, órgano dependiente del CNI. El objetivo del ENS es «establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información»[24].

Las Fuerzas Armadas también han sentido la necesidad de cubrir este aspecto de la defensa nacional. Desde hace algunos años, los diversos ejércitos han creado unidades dedicadas a tal fin. Con el objetivo de aunar esfuerzos, el Ministro de Defensa creó, el 19 de febrero del año pasado, el *Mando Conjunto de Ciberdefensa de las Fuerzas Armadas,* designando Comandante Jefe del mismo al General del Ejército del Aire López de Medina (figura 18), con la misión de realizar «el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional»[25].

El último paso dado por el Gobierno español en este campo ha sido la creación, el pasado 14 de febrero, del Consejo de Ciberseguridad Nacional, órgano encargado de la coordinación de las distintas administraciones del Estado en sus actuaciones para garantizar el uso seguro de las redes y sistemas de información mediante el fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques. El Consejo de Ciberseguridad Nacional está constituido por Presidencia del Gobierno, con el Centro

---

[24] http://en.wikipedia.org/wiki/United_States_Cyber_Command. [Último acceso: 08 September 2014]. «ccn-cert.cni.es,» Centro Criptológico Nacional , 2013. [En línea]. Available: https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=211&lang=es. [Último acceso: 28 July 2014].

[25] MORENES, P., *Boletin Oficial de Defensa,* Madrid: Ministerio de Defensa, 19 February 2013.

Nacional de Inteligencia (CNI), y los Ministerios de Interior, Defensa e Industria. Su presidencia será rotatoria por un periodo de un año y el primer responsable es actualmente el director del CNI, General del Ejército Félix Sanz Roldán.

Como se puede apreciar, gran parte de las acciones en el campo del ciberespacio están enfocadas hacia la defensa de la nación. Al igual que en el resto de países de nuestro ámbito, no se contemplan las acciones ofensivas. Todos, excepto Estados Unidos, dado que el Presidente Obama (figura 19) emitió, hace aproximadamente un año, una orden ejecutiva por la que se permitían acciones ofensivas, buscando mejorar la protección de la infraestructura y las industrias críticas del país de los ciberataques.

Figura19. Presidente Barack Obama con el Secretario de Defensa Leon Panetta en el Pentágono.

Los estados del arco oriental como China, Rusia y Corea del Norte, es bien sabido que realizan acciones ofensivas desde hace tiempo, sin necesidad de autorizarlas.

CONCLUSIONES

Las acciones delictivas en el ámbito de las telecomunicaciones dieron comienzo hace algunas décadas.

Con la aparición y el auge de Internet, variaron estas acciones hacia otros escenarios. El enfoque, en aquellos momentos, décadas de los 80 y 90, era del más puro espíritu romántico, sin otra mayor aspiración que la de superar los retos que suponían las barreras que había que franquear.

Cuando el uso del microprocesador se introdujo en todos los sistemas, hacia finales de los 90 y hasta nuestros días, los delitos en el ciberespacio tomaron otro carisma.

Comenzaron a realizarse acciones en el ciberespacio, donde naciones atacaban a otras naciones, normalmente como acciones de acompañamiento de confrontaciones armadas tradicionales.

Pronto estos ataques saltaron del ciberespacio para atacar a infraestructuras críticas de los países, a través de sistemas SCADA de gobierno y control de las infraestructuras, con los perjuicios y desastres que esto puede llegar a provocar.

Tanto unos como otros, los diferentes tipos de ataque tienen una serie de características comunes a ambos:

- son difícilmente atribuibles, por lo que sus autores niegan siempre su implicación.
- no se necesitan grandes medios para su realización, lo que implica que también son económicos.
- normalmente, aunque resulte paradójico, se realiza por una nación con una fuerza mayor contra otra menor.
- Los principales activos atacados son, normalmente, los sectores bancarios, gubernamentales y los medios de información.
- las naciones no despliegan todo su potencial cibernético, reservándolo para cuando sea verdaderamente necesario.

Las naciones se han protegido últimamente contra estas nuevas formas de acción creando policías especializadas e incluso ejércitos. Los servicios de inteligencia también están implicados.

Lo que el futuro deparará en este campo es muy prometedor, a la vez que impredecible.

[i]

*José Luis Aznar Lahoz**
Mando Conjunto de Ciberdefensa
Grupo Técnico (I+D+i) de la Jefatura de Operaciones