ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

40/2013 3 julio de 2013

Mª José Caro Bejarano

LA NUEVA DIMENSIÓN DE LA AMENAZA GLOBAL: LA AMENAZA CIBERNÉTICA

LA NUEVA DIMENSIÓN DE LA AMENAZA GLOBAL: LA AMENAZA CIBERNÉTICA

Resumen:

En los últimos 20 años, las tecnologías de la información y la comunicación se han desarrollado enormemente. Lo que empezó siendo una herramienta para ayudar a optimizar los procesos administrativos, es ahora un instrumento estratégico en la industria, la administración y la defensa. En este sentido, los Estados, las organizaciones internacionales y la industria buscan la manera de proteger sus activos de las ciberamenazas, no solo de manera reactiva sino preventiva.

Abstract:

In the past 20 years, information and communication technologies have developed greatly. What began as a tool to help office processes, it is now a strategic tool in industry, administration and defense. In this regard, States, international organizations and industry seek ways to protect their assets from cyber threats, not just in reactive but preventive way.

Palabras clave:

Ciberamenaza, ciberdefensa, tecnologías de la información y comunicación.

Keywords:

Cyber threat, cyber defense, information and communication technology.

LA NUEVA DIMENSIÓN DE LA AMENAZA GLOBAL: LA AMENAZA CIBERNÉTICA

En los últimos 20 años, las tecnologías de la información y la comunicación se han desarrollado enormemente. Lo que empezó siendo una herramienta para ayudar a optimizar los procesos administrativos, es ahora un instrumento estratégico en la industria, la administración y la defensa. Hace una década, los riesgos del ciberespacio y los retos a la seguridad sólo se discutían en pequeños grupos de expertos técnicos. Sin embargo, desde el 11S se hizo evidente que el mundo cibernético implica vulnerabilidades serias para las sociedades cada vez más interdependientes.

EVOLUCIÓN DE LA CIBERAMENAZA

Al igual que la llamada telaraña mundial o World Wide Web, inventada sólo hace un par de décadas, ha ido evolucionando, también lo han hecho las amenazas a que se enfrenta. Así, tanto gusanos como virus y otros códigos dañinos, se han transformado de simples molestias a problemas de seguridad graves y perfectos instrumentos de ciberespionaje.

Los ataques distribuidos de denegación de servicio (DDOS), que hasta ahora se veían básicamente como una forma de bloqueo on-line, se han convertido en una herramienta de guerra de información.

El código dañino "Stuxnet" aparecido públicamente en junio de 2010, estaba dirigido contra el programa nuclear iraní. Stuxnet mostró el riesgo potencial de malware que afecta a sistemas informáticos críticos que gestionan suministros de energía.

Con esto las primeras advertencias de los expertos desde el 11 de septiembre de 2001 sobre que, al igual que aviones, cualquier otro instrumento puede usarse como arma, se han convertido en realidad, lo que sugiere que la dimensión cibernética, tarde o temprano se podría usar para ataques graves con consecuencias mortales en el mundo físico.

EL CONTEXTO DE LA OTAN

Durante la crisis de Kosovo, la OTAN se enfrentó a sus primeros incidentes graves de ciberataques. Ejemplo de ello fue el bloqueo durante varios días de la cuenta de correo electrónico de la Alianza para los visitantes externos, y la reiterada interrupción de la página web de la OTAN.

No obstante, en aquel tiempo, la dimensión cibernética del conflicto se vio simplemente como un obstáculo a la campaña de información de la OTAN. Los ciberataques se vieron como un riesgo, pero limitado en su alcance y daño potencial, y sólo se requirieron unas respuestas técnicas limitadas acompañadas de actividades de información pública de baja

intensidad.

Los eventos del 11S cambiarían esa percepción. Pero aún más lo harían los incidentes de Estonia del verano de 2007 que constituyeron una fuente creciente de amenazas para la seguridad pública y la estabilidad del Estado. Los ciberataques masivos durante tres semanas mostraron que los países miembros de la OTAN, altamente dependientes de las comunicaciones electrónicas, también eran extremadamente vulnerables en el frente cibernético.

Esta creciente toma de conciencia sobre la gravedad de la amenaza cibernética se vio reforzada por incidentes en los años siguientes.

En 2008, uno de los ataques más graves hasta la fecha se lanzó contra los sistemas informáticos militares estadounidenses. A través de una sencilla memoria USB conectada a un ordenador portátil en una base militar en Oriente Medio, un software espía se extendió en sistemas clasificados y no clasificados sin ser detectado. Este software estableció el equivalente a una cabeza de puente digital, desde donde se transfirieron miles de archivos de datos a servidores bajo control extranjero.

Desde entonces, el ciberespionaje se ha convertido en una amenaza casi constante. Incidentes similares han ocurrido en casi todos los países de la OTAN. Hace un par de años en Estados Unidos, se vieron afectadas más de 72 compañías, incluyendo 22 oficinas del gobierno y 13 contratistas de defensa.

Estos incidentes, numerosos en los últimos siete a ocho años equivalen a una transferencia, sin precedentes históricos, de la riqueza y los secretos nacionales mejor guardados, básicamente a manos anónimas y, lo más probable, maliciosas.

Durante el conflicto entre Georgia y Rusia, los ataques masivos a sitios web y servidores del gobierno de Georgia, dieron al término de ciberguerra una forma más concreta. Aunque estas acciones no hicieron ningún daño físico real, sin embargo, debilitaron al gobierno de Georgia durante una fase crítica del conflicto. Estos ataques también tuvieron un impacto en su capacidad para comunicarse con la población nacional, y también mundial.

El gusano Stuxnet aparecido en 2010 señaló un salto cualitativo en las capacidades destructivas de la ciberguerra. En el verano de 2010 se supo que alrededor de 45.000 sistemas de control industrial de Siemens de todo el mundo habían sido infectados por un código malicioso, que podía manipular los procesos técnicos críticos de las plantas de energía nuclear de Irán. Aunque la evaluación de los daños no estuvo clara, esto demostró el

riesgo potencial del malware que afecta a los sistemas informáticos críticos de gestión de los suministros de energía o las redes de tráfico. Por primera vez, aquí estaba la prueba de que los ciberataques podían causar daño físico real y poner en riesgo vidas humanas.

Una equilibrada evaluación de la amenaza

Estos hechos dejaron claro dos cuestiones:

- hasta el momento, los actores más peligrosos del ciber-dominio siguen siendo los Estados. A pesar de una mayor disponibilidad de la capacidad ofensiva en las redes criminales que podrían también ser utilizados en el futuro por actores no estatales, como terroristas, el espionaje y el sabotaje altamente sofisticado en el ciber-dominio todavía necesita las capacidades, la determinación y la justificación del coste-beneficio de un Estado.
- Los daños físicos y el ciberterrorismo real no ha tenido lugar todavía. Pero la tecnología de los ciberataques está evolucionando claramente de una simple molestia a una amenaza seria contra la seguridad de la información e incluso la infraestructura crítica nacional.

No hay ninguna duda de que algunos países ya están invirtiendo masivamente en capacidades cibernéticas que pueden usarse con fines militares. A primera vista, la carrera armamentista digital se basa en una lógica clara e ineludible, ya que el dominio de la ciberguerra ofrece numerosas ventajas: es asimétrica, atractivamente barata, además de todas las ventajas que inicialmente están en el lado del atacante.

Además, prácticamente no hay disuasión efectiva en la ciberguerra, ya que incluso la identificación del atacante es extremadamente difícil y, cumpliendo con el derecho internacional, probablemente casi imposible. Bajo estas circunstancias, cualquier forma de represalia militar sería muy problemática, tanto en términos jurídicos como políticos.

Por otro lado, sin embargo, las capacidades de ciberdefensa han evolucionado igualmente y la mayoría de las naciones occidentales han reforzado considerablemente sus defensas en los últimos años. La buena ciberdefensa permite gestionar estas amenazas, en la medida en que los riesgos residuales sean aceptables, igual que sucede con las amenazas clásicas.

Pero en lugar de hablar de la ciberguerra como una guerra en sí misma – evocando el "Digital Pearl Harbour" o el "11S cibernético" - sería mucho más apropiado describir los ciberataques como uno de los muchos medios para hacer la guerra. Los riesgos de los ciberataques son muy reales y cada vez más grandes. Al mismo tiempo, tampoco hay razón

para el pánico, ya que en el futuro inmediato estas amenazas no serán apocalípticas ni completamente inmanejables[1].

Enfrentándose al desafío

La OTAN continúa con su adaptación a este nuevo tipo de desafío a la seguridad. Un año después del 11S, la OTAN emitió un llamamiento importante para mejorar sus "capacidades para defenderse de los ciberataques", como parte del Compromiso de Capacidades que se acordó en Praga en noviembre de 2002. No obstante, en los años posteriores, la Alianza se concentró principalmente en la aplicación de las medidas de protección pasiva solicitadas por el lado militar.

Los acontecimientos de Estonia de la primavera de 2007 llevaron a la Alianza a repensar radicalmente su necesidad de una política de ciberdefensa e impulsar sus medidas de lucha a un nuevo nivel. De ese modo, la Alianza, elaboró por primera vez una "Política de Ciberdefensa", aprobada en enero de 2008, que estableció tres pilares fundamentales en la política de la Alianza en el ciberespacio:

- La subsidiariedad, es decir, la asistencia se proporciona sólo a petición, de lo contrario, se aplica el principio de la soberanía de los estados con su responsabilidad propia;
- No duplicación, es decir, evitar la duplicación innecesaria de las estructuras o capacidades en los planos internacional, regional, y nacional;
- Seguridad, es decir, la cooperación basada en la confianza, teniendo en cuenta la sensibilidad de la información de los sistemas que debe hacerse accesible y sus posibles vulnerabilidades.

Esto constituyó un salto cualitativo. También allanó el camino para la decisión fundamental adoptada en Lisboa para proseguir de forma continuada con la ciberdefensa como un elemento independiente en la agenda de la OTAN.

Con las decisiones adoptadas en Lisboa en noviembre de 2010, la Alianza estableció con éxito las bases para un examen de esta cuestión. De este modo, la OTAN no sólo proporcionaba una actualización muy necesaria a las estructuras existentes como la capacidad de respuesta ante incidentes, sino que también comenzaba de forma conjunta,

1 Según el *Dr. Olaf Theiler, especialista nacional en la División de Operaciones de la OTAN en el cuartel general en Bruselas.*

como una alianza, a enfrentarse a los retos, muy reales y en crecimiento, de ciberdefensa.

En consonancia con el nuevo Concepto Estratégico, se revisó la Política de Ciberdefensa que define las amenazas informáticas como una fuente potencial para la defensa colectiva de conformidad con el artículo 5 de la OTAN. Por otra parte, la nueva política - y el Plan de Acción para su aplicación - proporciona a las naciones de la OTAN, directrices claras y una lista consensuada de las prioridades al adoptar la ciberdefensa, incluida una mayor coordinación dentro de la OTAN, así como con sus socios.

El 8 de junio de 2011, los ministros de Defensa de la OTAN aprobaron la revisión de la Política de Ciberdefensa, política que establece una visión clara de los esfuerzos en ciberdefensa en toda la Alianza, y un Plan de Acción asociado a su aplicación. En octubre de 2011, los ministros acordaron los detalles de ese Plan de Acción. Esta revisión de la política ofrece un enfoque coordinado de ciberdefensa mediante la prevención de ciberataques y la construcción de resiliencia.

En febrero de 2012, se firmó un contrato de 58 millones de euros para establecer una Capacidad de Respuesta ante Incidentes Informáticos (NCIRC), que estará plenamente operativo en octubre de 2013. También se creó una célula de Concienciación de Ciberamenazas para mejorar el intercambio de inteligencia y la concienciación de esta situación.

En abril de 2012, la ciberdefensa se integró en el Proceso de Planificación de Defensa de la OTAN (NDPP). El objetivo era identificar las necesidades de ciberdefensa relevantes y priorizados por la NDPP.

En mayo de 2012 en Chicago los jefes de Estado y de Gobierno reafirmaron su compromiso de mejorar las ciberdefensas de la Alianza protegiendo todas sus redes de forma centralizada y aplicando los elementos críticos de la capacidad operativa plena del NCIRC en octubre de 2013.

El 1 de julio de 2012, en el contexto de la reforma de las agencias de la OTAN, se estableció la agencia OTAN de Comunicación e Información (NCI). La agencia facilitará incorporar a todos los organismos de la OTAN bajo protección centralizada y proporcionará beneficios operacionales y ahorros de costes a largo plazo.

En abril de 2013, se cumplió un hito fundamental cuando la infraestructura de gestión de la red central de defensa y la capacidad analítica se instaló en el centro técnico NCIRC de Mons, Bélgica.

El 4 de junio de 2013, en su primera reunión dedicada a la ciberdefensa, los ministros de Defensa de la OTAN acordaron que la capacidad de ciberdefensa de la Alianza debería estar plenamente operativa en otoño. Esto incluye la creación de equipos de reacción rápida para ayudar a proteger los propios sistemas de la Alianza. La protección se extenderá para entonces a todas las redes de propiedad y operadas por la Alianza. Los ministros de Defensa también acordaron continuar las conversaciones en la próxima reunión de octubre sobre el apoyo y asistencia de la OTAN a los aliados que soliciten ayuda ante un ciberataque.

EL CONTEXTO NACIONAL

En el contexto español el Ministerio de Defensa creó el pasado mes de febrero el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas para hacer frente a las amenazas a España procedentes de Internet. Este mando alcanzará su capacidad operativa inicial este verano, según anunció el Jefe de Estado Mayor de la Defensa (Jemad), Almirante Fernando García Sánchez.

Este nuevo mando de lucha contra potenciales ciberataques depende directamente del Jemad. El ciberespacio es un campo más en el que han de trabajar las Fuerzas Armadas, junto a los tradicionales. Según el Jemad, este mando habrá alcanzado su capacidad definitiva a finales de 2013 o, como mucho, el primer semestre de 2014.

Este cibermando viene a ser el equivalente del US Cyber Command, creado por el Pentágono en 2009 para enfrentarse en lo que Washington definió como el "campo de batalla del futuro".

La propia revisión de la Estrategia de Seguridad Nacional[2] aprobada por el Gobierno en mayo de este año considera el ciberespacio como un “nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas”.

EL CONTEXTO INTERNACIONAL

En el contexto internacional actual parece que la mayor amenaza proviene de la delincuencia organizada, cuya dedicación es básicamente la obtención de beneficio

2 Disponible en http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/Estrategia_Seguridad_Nacional_2013.pdf

económico. Utilizan una infraestructura en red con un modelo sin jerarquía, donde existen diferentes grupos que comercializan información valiosa del tipo financiero, código dañino, exploits, troyanos, etc., y que están orientados a cometer delitos, ya sea para la obtención de dinero, datos o información. Es el conocido "Crime as a Service, CaaS", mercados negros virtuales del crimen sin fronteras físicas, donde es muy difícil la reacción con medios tradicionales. De ahí que tanto la prevención como la detección sean fundamentales. En este mercado de la delincuencia organizada se reparten los papeles, donde unos crean el código dañino, otros ejecutan el ataque y otros recogen el dinero mediante una estructura de "mulas".

Las últimas noticias de los medios de comunicación han puesto en evidencia la importancia y permanencia del espionaje incluso entre Estados, con acusaciones de espionaje de EE.UU. hacia China y viceversa, de EE.UU. hacia países europeos y a otros aliados, y de otros países hacia países occidentales.

El espionaje, si es industrial, supone una amenaza real al activo principal de una empresa, su conocimiento y propiedad industrial, cuya pérdida, si va a para a la competencia puede suponer la quiebra total de la empresa.

Todo esto bajo la preocupación de la pérdida de privacidad de los ciudadanos frente a las grandes corporaciones de tecnologías de la información y comunicaciones, de carácter global, y frente a las cuales las normas nacionales de protección de datos parecen no tener suficiente capacidad de reacción.

Mª José Caro Bejarano
Analista Principal IEEE