ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

32/2012 25 julio de 2012

María José Caro Bejarano

PROGRESA LA DEFENSA CIBERNÉTICA DEL REINO UNIDO

PROGRESA LA DEFENSA CIBERNÉTICA DEL REINO UNIDO

Resumen:

El Reino Unido avanza en su defensa cibernética. Era uno de los compromisos de la Estrategia de Seguridad Británica de octubre de 2010. La amenaza cibernética está identificada como riesgo de nivel I.

Según un informe presentado ante el parlamento británico el pasado 13 de julio por el Comité de Inteligencia y Seguridad, el Reino Unido debe prepararse para participar en una serie de operaciones ofensivas cibernéticas para proteger los intereses de su seguridad nacional.

Abstract:

The United Kingdom advances its cyber defense. It was one of the commitments of the National Security Strategy of October 2010. The cyber threat is identified as a Tier One risk. According to a report presented to the British Parliament on July 13th by the Intelligence and Security Committee, the UK must be prepared to engage in a range of offensive cyber operations to protect national security interests.

Palabras clave:

Reino Unido, ciberseguridad, amenaza cibernética, estrategia de ciberseguridad.

Keywords:

United Kingdom, cyber security, cyber threat, cyber security strategy.

PROGRESA LA DEFENSA CIBERNÉTICA DEL REINO UNIDO

El Reino Unido avanza en la defensa ante la amenaza cibernética identificada como prioritaria en su Estrategia de Seguridad Nacional de octubre de 2010.

Según un informe presentado ante el parlamento británico el pasado 13 de julio por el Comité de Inteligencia y Seguridad, el Reino Unido debe prepararse para participar en una serie de operaciones ofensivas cibernéticas para proteger los intereses de su seguridad nacional. [1]

La amenaza cibernética está identificada como uno de los cuatro riesgos de nivel I de la Estrategia de Seguridad Británica[2], publicada en octubre de 2010.

La Estrategia de Seguridad Británica, como principal aportación, aplica una metodología de valoración del riesgo de la seguridad nacional en un horizonte de cinco a veinte años, agrupando los riesgos o amenazas en tres niveles y 15 tipos priorizados según la probabilidad de ocurrencia y el impacto relativo. Los riesgos del nivel I (de mayor probabilidad e impacto) son los que se consideran en el período de aplicación de la Estrategia de cinco años. Esta valoración se revisa cada dos años. La Estrategia pretende predecir, prevenir y mitigar los riesgos a la seguridad, con los recursos disponibles, actuando para reducir la probabilidad de ocurrencia y desarrollando las capacidades necesarias para mitigar su impacto.

Dentro del grupo de nivel I se encuentran los siguientes riesgos:

- Terrorismo internacional que afecte al Reino Unido o a sus intereses, incluyendo un ataque químico, biológico, radiológico o nuclear; y/o un aumento importante en niveles de terrorismo en Irlanda del Norte.
- ataque hostil sobre el ciberespacio nacional por otros Estados o por el crimen organizado
- un accidente importante o un desastre natural que precisa una respuesta nacional, tales como inundaciones costeras que afecten a tres o más regiones del país, una pandemia de gripe.
- Una crisis militar internacional entre estados, afectando al país y sus aliados, así como a actores estatales y no estatales.

[1] Véase "UK should engage in offensive cyber operations, say MPs". Eleanor Keymer. IHS, 2012.
[2] El documento de análisis 18/2010 del IEEE analiza la Estrategia de Seguridad Británica en www.ieee.es/Galerias/fichero/docs_analisis/2010/DIEEEA18-2010EstrategiaNacionalSeguridadBritanica.pdf

La inclusión de la amenaza cibernética en el grupo de Nivel I obedecía a la advertencia que hizo en 2010 el director del Centro de Comunicaciones Gubernamental (GCHQ), de que las amenazas cibernéticas son "reales y creíbles" y de que las redes del gobierno eran el blanco de más de 1.000 correos electrónicos maliciosos al mes.

El mencionado informe afirma que las agencias británicas militares y las de inteligencia y seguridad deben involucrarse en los ataques cibernéticos de represalia cuando las redes del país estén en peligro: es el caso del acceso a los datos o a redes por parte de los atacantes cibernéticos para "obtener inteligencia o de provocar un efecto sin ser detectado"; la alteración de los sistemas por los atacantes; el uso de las capacidades cibernéticas para realizar operaciones de información y destruir datos, redes o sistemas como apoyo a conflictos bélicos. [3]

El informe menciona el virus Stuxnet como un ejemplo de alteración de las redes de los adversarios. Se trata de un gusano informático que se utilizó para alterar el programa de enriquecimiento de uranio de Irán – aunque el informe señala que las agencias del Reino Unido no participaron en la operación.[4]

Este informe declara que, aunque el Reino Unido ha progresado en el desarrollo de las capacidades cibernéticas, queda mucho trabajo por hacer ya que "los retrasos en el desarrollo de estas capacidades dan la ventaja a los enemigos". [5]

El Comité elogió la labor del Grupo de Seguridad de Comunicaciones y Electrónica -en el Reino Unido (CESG en sus siglas en inglés[6]) y los organismos asociados como "altamente valorado por los sectores público y privado". Sin embargo, el comité hizo hincapié en la importancia de establecer un modelo de financiación a largo plazo para el CESG que sigue sufriendo escasez de fondos y ha sido subvencionado por el Centro Gubernamental de Comunicaciones (GCHQ en sus siglas en inglés[7]) por "varios millones de libras al año".

[3] Véase nota 1.
[4] Según 'The Washington Post' la Agencia de Seguridad Nacional (NSA) de EE UU, la CIA y representantes militares de Israel participaron en una campaña que incluye el uso del destructivo virus Stuxnet, que causó fallos en las centrifugadoras de la planta secreta de enriquecimiento de uranio de Natanz (Irán) en 2010, junto con la creación del virus de espionaje Flame, un sofisticado programa diseñado para captar información clave y sabotear el polémico programa nuclear iraní y detectado el pasado junio. Véase más información en el documento informativo 34/2012 del IEEE "Flame: una nueva amenaza de ciberespionaje" en: www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI342012_Flame_Ciberespionaje_MJCB.pdf
[5] Véase nota 1.
[6] Communications-Electronics Security Group, CESG.
[7] Government Communications Headquarters, GCHQ.

Ya se han invertido 650 millones de libras esterlinas, (unos 834 millones de euros) en la mejora de las capacidades cibernéticos del país. Más de la mitad de la financiación de este Programa Nacional de Seguridad Cibernética se asignó a las agencias de inteligencia, en su mayor parte al GCHQ. Este financiación se invertido en: ampliar la labor de asesoramiento en protección de la seguridad cibernética y en aseguramiento de la información (Information Assurance, en su acepción inglesa); en mejorar la detección y análisis de los ataques cibernéticos; en aumentar la cooperación con países aliados; y en la creación de una unidad cibernética conjunta en colaboración con el Ministerio de Defensa para desarrollar nuevas tácticas, técnicas y planes relativos a las operaciones militares.

Refiriéndose a la colaboración internacional y a la necesidad de un acuerdo de los gobiernos que actúan adecuadamente en el ciberespacio y en cumplimiento con el derecho internacional, el secretario de Relaciones Exteriores del Reino Unido, William Hague, dijo al comité que ya se habían realizado progresos en la Conferencia sobre el ciberespacio celebrada en Londres en noviembre de 2011.

El comité también señaló la importancia de una "higiene" cibernética, ya que el GCHQ estima que el 80 por ciento de todos los ataques cibernéticos podrían evitarse si las organizaciones invierten en el software de seguridad adecuado, y emplean contraseñas 'fuertes' y mediante la formación de los usuarios.

Centrándonos en el ámbito nacional, la Estrategia Española de Seguridad[8] aprobada el 24 de junio de 2010 contempla "Los potenciadores del riesgo" en el capítulo 3, y entre ellos los "Peligros tecnológicos", de los cuales destaca la amenaza en el ciberespacio: "La ciberseguridad, relacionada con las infraestructuras vitales para el funcionamiento de un país, se ha convertido en un ámbito clave para la seguridad de cualquier Estado." De las Amenazas, Riesgos y Respuestas tratadas en el Capítulo 4 menciona las Ciberamenazas**: "**Los *ciberataques* son una amenaza en crecimiento con la que los posibles agresores -terroristas, crimen organizado, empresas, Estados o individuos aislados- podrían poner en dificultad infraestructuras críticas". Para luchar contra ellas establece unas Líneas estratégicas de acción (véase pg. 66).

Una de las iniciativas que propone la Estrategia Española es la "Elaboración coordinada de las Estrategias de segundo nivel necesarias para el desarrollo de la Estrategia Española de Seguridad, entre ellas una Estrategia Española de *Ciberseguridad"*. Dicha Ciberestrategia se

[8] La Estrategia Española de Seguridad se puede consultar en www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/EstrategiaEspanolaSeguridad_junio2011.pdf

encuentra en proceso de elaboración y aprobación.

A nivel europeo la Ciberseguridad también es una preocupación. Recientemente la Agencia Europea de Seguridad de las Redes y la Información (ENISA) ha publicado el informe "Estrategias Nacionales de Ciberseguridad"[9] en el que incluye un breve análisis de la situación actual de las estrategias de seguridad cibernética en la Unión Europea. Identifica los temas comunes y las diferencias, por último concluye con una serie de observaciones y recomendaciones.

El documento se basa en el análisis de los resultados preliminares de un proyecto en el que ENISA está trabajando para desarrollar una guía de buenas prácticas sobre cómo desarrollar, implementar y mantener una Estrategia Nacional de Seguridad Cibernética. La Guía de Buenas Prácticas pretende ser una herramienta útil para proporcionar consejos prácticos a los responsables e involucrados en las estrategias de seguridad cibernética.

María José Caro Bejarano
Analista del IEEE

[9] Informe ENISA: Estrategias Nacionales de Ciberseguridad