ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

78/2012 27 diciembre de 2012

Mª José Caro Bejarano

DE LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL

DE LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL

Resumen:

La ciberseguridad aparece hoy en la mayoría de estrategias de seguridad nacional como uno de los factores clave en la protección de las infraestructuras críticas nacionales. En contraste con las primeras etapas de las ciberamenazas, lo que surgió como una amenaza en el terreno de la delincuencia y del sector empresarial, se ha fundido con el enfoque orientado a la protección de las redes gubernamentales y de las infraestructuras esenciales para el bienestar económico y social de la sociedad.

Abstract:

Cybersecurity appears nowadays in most national security strategies as one of the key factors in protecting national critical infrastructures. In contrast to the early stages of cyber threats, which emerged as a threat in the field of crime and the business sector, has merged with the approach oriented to the protection of government networks and key critical infrastructures for economic and social well-being of the entire society.

Palabras clave:

Seguridad Nacional, ciberseguridad, ciberamenazas, protección de infraestructuras críticas.

Keywords:

National security, cyber security, cyber threats, critical infrastructure protection.

LA EVOLUCIÓN DE LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL

Every American depends – directly or indirectly – on our system of information networks. They are increasingly the backbone of our economy and our infrastructure; our national security and our personal well-being. … As President, I'll make cyber security the top priority that it should be in the 21st century.

(Remarks of Senator Barack Obama – as prepared for delivery,
Summit on Confronting New Threats, Purdue University, 16 July 2008)

"Ciber" es un prefijo derivado de la palabra cibernética y ha adquirido el significado general "mediante el uso de un ordenador". También se usa como sinónimo de ciberespacio. El ciberespacio tiene la connotación de unión de todas las redes de comunicación, bases de datos y fuentes de información en un vasto, enmarañado y diverso manto de intercambio electrónico. Este entorno existe allí donde hay cables de teléfono, cables coaxiales, fibra óptica y ondas electromagnéticas[1].

La ciberseguridad se ocupa de hacer seguro este entorno. Se refiere a un conjunto de actividades y medidas, técnicas y no técnicas, orientadas a proteger la "geografía real" del ciberespacio, pero también los dispositivos, software, y la información o datos que contiene o comunica, de todas las posibles amenazas. Amenazas que podrían potencialmente dañar la información y que se clasifican en fallos, accidentes y ataques, aun cuando estas categorías no son necesariamente mutuamente excluyentes o fácilmente distinguibles[2]. Los fallos son causados por deficiencias en el sistema o en un elemento externo del cual depende, pueden deberse a errores de diseño en el software, degradación del hardware, error humano o datos dañados o corrompidos. Los accidentes incluyen el rango completo de eventos de ocurrencia aleatoria y potencialmente dañinos como los desastres naturales. Normalmente los accidentes son eventos generados externamente, es decir fuera del sistema, mientras que los fallos son eventos internos. Por último, los ataques son organizados por un adversario. Esta clasificación, aunque no es necesariamente la más importante en términos de frecuencia de ocurrencia o impacto, es de principal importancia en el debate por la dimensión de los actores.

La intrusión en un sistema puede ser el principal objetivo del ataque y también se considera el más peligroso, en comparación, por ejemplo, con la denegación de servicio que es menos

[1] Dyson et al, 1994
[2] Ellison et al. 1997; Whitman y Mattord 2002
Se puede consultar la web http://www.afpc.org.

dañino por el efecto que produce en el sistema. Si un intruso consigue el control completo del sistema o los derechos del administrador, tiene acceso sin restricción a todo el sistema. Un intruso puede retrasar, alterar, corromper, aprovecharse, destruir, robar y modificar la información.

Se puede argumentar que la ciberseguridad y la seguridad nacional no difieren en su esencia, ambas tienen la connotación de ser la condición de estar libre de peligro (real o imaginado). La palabra seguridad generalmente se usa como sinónimo de "estar seguro", pero el término técnico seguridad significa no sólo que algo es seguro, sino que se ha hecho seguro. Es decir, se refiere al grado de protección que resulta de la aplicación de ciertas actividades y medidas. Por tanto, la noción de seguridad incluye la práctica de hacer algo seguro "securizándolo". Es por tanto, un estado y una actividad, práctica o proceso. Puede decirse que la ciberseguridad y la seguridad nacional están sometidas al mismo tipo de amenaza, desde terroristas hasta otros Estados.

Sin embargo, la ciberseguridad y la seguridad nacional difieren en el ámbito, en términos de los actores involucrados y en el objeto a proteger. Mientras la seguridad de los sistemas de información, en sentido estricto, se refiere a medidas técnicas para asegurar los flujos de información, las medidas de seguridad nacional incluyen mucho más, como el mantenimiento de las fuerzas armadas, el mantenimiento de los servicios de inteligencia para detectar amenazas y medidas de defensa civil. Sin embargo, con la incorporación de la ciberseguridad a la agenda de la política de seguridad, las dos nociones se entremezclan. La seguridad nacional intenta crear resiliencia (capacidad de resistencia y recuperación) y redundancia en las infraestructuras nacionales a través de medidas de ciberseguridad y la ciberseguridad se incluye como una prioridad principal en la agenda de seguridad nacional. Esto significa que las medidas que generalmente se consideran en el ámbito de la seguridad de la información pueden ahora incluirse entre las medidas que garantizan la seguridad nacional y viceversa.

La amenaza a la ciberseguridad se centró inicialmente en la ciberdelincuencia y ataques a empresas. Después surgió la preocupación por la protección de las redes gubernamentales y la información clasificada almacenada en ellas. Esto abrió el debate sobre si "seguridad" se refería a la seguridad de la sociedad como un todo, o si solo se refería a la seguridad de usuarios individuales o sistemas técnicos y por tanto, debería ser gestionado por autoridades distintas a los organismos de seguridad nacional.

A mitad de los años 90, el tema de la ciberseguridad empezó a aparecer más firmemente en la agenda de política de la seguridad por su interrelación con el terrorismo y la protección de

infraestructuras críticas. Durante aquel tiempo se estableció que los sectores clave de la sociedad moderna, incluyendo aquellos vitales para la seguridad nacional y para el funcionamiento esencial de las economías industrializadas, descansan en un amplio espectro de sistemas de control basados en software interdependientes nacionales e internacionales. Estas infraestructuras críticas de la información (ICI), son la base de muchos elementos de las infraestructuras críticas (IC), como muchas tecnologías de la información y las comunicaciones (TIC) que conectan otros sistemas de infraestructuras de forma interrelacionada e interdependiente. Esto sirvió para aclarar que la ciberseguridad es una de las herramientas clave para proteger los recursos esenciales nacionales.

A finales de los años 80 y principios de los 90, comenzaron a aparecer documentos en EE.UU. que establecían una clara conexión entre ciberamenazas, ciberseguridad e infraestructuras críticas. Algunas publicaciones avisaban que la revolución de la era de la información había convertido a EE.UU. en vulnerable de forma asimétrica, debido a la desaparición de fronteras y a la dependencia de las fuerzas militares de infraestructuras civiles vulnerables.

Con el crecimiento y extensión de la redes de ordenadores a muchos más aspectos de la vida, cambió el objeto de la protección. Mientras anteriormente se había insistido en proteger las redes gubernamentales, ahora se trataba del conjunto de la sociedad. De este modo las ciberamenazas pueden considerarse como una amenaza a los valores del núcleo de al sociedad, y al bienestar económico y social de un país, y la ciberseguridad como una tarea esencial de la seguridad nacional en la protección de las infraestructuras críticas.

Debido a la creciente importancia de la información y conocimiento que reside en el sector privado, propietario o gestor de la misma, y dado que en las sociedades liberales no es una opción válida una intervención intrusiva en el mercado, al estado solo le queda una opción: intentar acordar con el sector privado algún tipo de responsabilidad. Esta llamada a la cooperación con el sector privado debería legitimarse bajo el argumento convincente de que los intereses de seguridad nacional y del sector privado son los mismos. Los mundos de la economía y la seguridad están más unidos hoy que nunca. El aspecto clave en este campo busca convencer a la comunidad empresarial de que la naturaleza interdependiente de las infraestructuras crea un entorno de riesgo compartido y que la gestión de ese riesgo requiere de una cooperación estrecha entre los sectores público y privado. Esto debe hacerse apelando a la responsabilidad: ya que las infraestructuras son gestionadas o son propiedad del sector privado, la garantía de las infraestructuras críticas es una responsabilidad compartida de ambos sectores, privado y público. Las amenazas son también compartidas, como el terrorismo, el espionaje industrial y la delincuencia organizada.

Por ello, la distinción entre las esferas de acción pública y privada ha desaparecido. Esto implica que la defensa nacional ya no es exclusiva del gobierno, y que la seguridad económica no es asunto exclusivamente del sector negocio. Se requiere una estrategia de compartición de información cooperativa hacia la otra parte que no la tiene: el gobierno puede ayudar recopilando y difundiendo información sobre los ataques o técnicas que pueden provocar un daño, y los propietarios y operadores de estas infraestructuras pueden ayudar informando al gobierno cuando se detecten nuevas herramientas o técnicas. Es decir, el gobierno informa de grupos o naciones potencialmente hostiles, mientras que el sector privado informa sobre conocimiento tecnológico que el sector público no tiene. Este enfoque plantea la idea de "seguridad distribuida" y "responsabilidad distribuida".

Mª José Caro Bejarano
Analista del IEEE