Ciberseguridad nacional, un asunto prioritario para España

Con el desarrollo de las tecnologías de comunicaciones, la Defensa Nacional, tradicionalmente centrada en las áreas de Tierra, Mar y Aire, debe cubrir un nuevo espacio en el que la rapidez y facilidad de los intercambios ha eliminado las barreras de distancia y tiempo. Este nuevo espacio relacional (el ciberespacio), en donde no existen fronteras y del que dependen cada día más las sociedades avanzadas, está sufriendo un incremento constante de los ataques y amenazas provenientes de muy diversos frentes. Por este motivo, es hora de desarrollar una Estrategia Nacional de Ciberseguridad que proteja las redes y sistemas de información de nuestro país y que tan cruciales son para la vida diaria de nuestros habitantes.

Javier Candau Romero

Según establece la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, la política de defensa tiene por finalidad la protección del conjunto de la sociedad española, de su Constitución, de los valores superiores, principios e instituciones que en ella se consagran, del Estado social y democrático de derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial de España. Esta Defensa, tal y como recoge la Directiva de Defensa Nacional (DDN) 1/2008, se debe enmarcar en una Estrategia de Seguridad Nacional que esté en consonancia con las estrategias adoptadas por las organizaciones internacionales a las que España pertenece y que garantice la protección de los intereses nacionales, respetando el marco constitucional y los tratados internacionales, y proporcionando a su vez una respuesta integral basada en el análisis de las amenazas y de las causas que las producen.

Por este motivo, es más que necesario tener en cuenta la Comunicación al Parlamento Europeo, lanzada el pasado 31 de marzo de 2011, por la Comisión Europea con el título: *"Sobre la protección de infraestructuras críticas de información. Logros y próximas etapas: hacia la ciberseguridad global"**. En ella, y entre otros aspectos, se reiteraba la ya conocida dependencia de las TIC que existe en nuestro continente (extrapolable a buena parte del mundo) desde el punto de vista social, político y económico, y al crecimiento constante en el número, intensidad, sofisticación e impacto potencial de las amenazas que se acechan sobre ellas. Textualmente, la Comisión aseguraba: *"están surgiendo amenazas nuevas y más avanzadas tecnológicamente, con una dimensión geopolítica que, de forma más clara, es de carácter mundial. Estamos presenciando una tendencia hacia el uso de TIC con fines de predominio político, económico y militar, incluida la capacidad ofensiva"*.

* COM(2011)163 final

En España, las responsabilidades de seguridad en el ciberespacio están distribuidas por varios organismos, tanto de la Administración General del Estado (AGE), como de la autonómica. Esta disgregación favorece los posibles solapes y redundancias en los ámbitos de actuación que impiden un tratamiento completo de los nuevos desafíos.

Estas **amenazas** podrían agruparse en distintas categorías, según los fines que persigan:

• Fines de **explotación**, como es el caso de las Amenazas Persistentes Avanzadas (APT) de espionaje político y económico (por ejemplo, GhosNet o "Aurora", considerada esta última como uno de los ataques dirigidos más sofisticados hasta ahora registrados, destinado al robo de información sensible), los robos de identidad, o los recientes ataques contra el sistema de comercio de derechos de emisión o contra los sistemas de TI de los Estados (Australia, la propia Comisión Europea, Francia o Estados Unidos figuran entre los más recientemente atacados).

• Fines de **perturbación**, como la denegación de servicio distribuido (DDoS) o el "spam" generado vía *botnets* (por ejemplo, la red Conficker, con más de siete millones de máquinas, o la red Mariposa, con base en España, con una red de 12,7 millones de máquinas"); "Stuxnet" (dejando claro que las infraestructuras críticas pueden ser atacadas con éxito), convocatorias de la organización Anonymous (que en España coordinó ataques contra el Ministerio de Cultura, la SGAE y diversos partidos políticos), o el corte de los medios de comunicación.

• Fines de **destrucción**; esta es una posibilidad que todavía no se ha presentado pero, vista la omnipresencia creciente de las TIC en las infraestructuras críticas (por ejemplo, en las redes inteligentes y los sistemas de distribución de agua), no cabe descartarla en los próximos años.

De igual forma, muchos Estados han declarado públicamente durante el año 2010 que el ciberataque puede ser empleado como una herramienta más de sus estrategias de inteligencia o militares; consecuentemente, la ciberdefensa también. En este sentido su objetivo final es tanto la exfiltración de información del enemigo como la inutilización o destrucción de los sistemas enemigos tanto para evitar el mando y control de sus fuerzas, como para causar daños en sus servicios esenciales y en su población. Es el mismo objetivo que la actividad de inteligencia que lo soporta: adquirir ventaja política, económica, comercial o militar con la información adquirida en los sistemas atacados.

La constatación clara de esta realidad es que en los últimos años se han detectado numerosos intentos de agresión, muchos de ellos exitosos, sobre sistemas sensibles de diferentes naciones en el ámbito de la UE y la OTAN. Como ejemplo, algunas naciones como Estados Unidos, Reino Unido, Alemania o Francia han declarado públicamente haber recibido ataques muy graves con impactos serios sobre la información sensible gestionada en los sistemas de sus respectivos Gobiernos. Seguramente muchos otros Gobiernos y empresas han recibido ataques similares que no se han hecho públicos.

De igual modo, se ha constatado que la actividad terrorista internacional emplea Internet como una herramienta más que le ayuda a cumplir sus objetivos (de momento, más como propaganda, reclutamiento y comunicaciones, aunque bien es cierto que se espera que, al igual que el crimen organizado, acabe por utilizarlo para la obtención de financiación).

Es necesario concebir una Estrategia Nacional de Ciberseguridad que persiga conseguir un ciberespacio más seguro, y al tiempo –tal y como han hecho otras naciones– dotar de presupuesto adecuado a las agencias con misiones en la seguridad de los sistemas TIC de la Administración y a las unidades encargadas del ciberdelito en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Ante esta alarmante situación, la OTAN ubicó los **atentados cibernéticos**, según su Estrategia publicada recientemente, entre las tres mayores amenazas del presente, junto con el terrorismo y las armas de destrucción masiva.

La defensa del ciberespacio

En un esfuerzo por abordar esta problemática, han sido y son muchos los países que han elaborado una estrategia nacional de ciberseguridad, que, al igual que en su versión "física" debe adoptar posturas ofensivas y defensivas en un espacio donde no hay barreras de distancia y de tiempo y en el que las fronteras nacionales están diluidas.

Reino Unido, Australia, Canadá, Alemania, Países Bajos, Francia o Estados Unidos (cuya revisión acaba de hacerse pública) son algunas de las naciones que han hecho públicas unas políticas de ciberseguridad y ciberdefensa más destacadas.

En España, las responsabilidades de seguridad en el ciberespacio están distribuidas por varios organismos, tanto de la Administración General del Estado (AGE), como de la autonómica. Así, los ministerios de Defensa, Interior, Industria, Política Territorial y Administración Pública, el Centro Nacional de Inteligencia o los Equipos de Respuesta a Incidentes (CERTs) de carácter nacional o autonómico, trabajan en el ámbito de la ciberseguridad. Esta disgregación en diferentes organismos, que además no tienen las mismas prioridades desde el punto de vista de la seguridad, favorece los posibles solapes y redundancias en los ámbitos de actuación que impiden un tratamiento completo de los nuevos desafíos del ciberespacio.

Es necesario, por tanto, concebir una Estrategia Nacional de Ciberseguridad que persiga conseguir un ciberespacio más seguro a través de los siguientes objetivos:

1.Establecer una línea de defensa común y homogénea. Para ello se debe desarrollar con la máxima rapidez el **Esquema Nacional de Seguridad** y mejorar el intercambio de información de agresiones y vulnerabilidades que se detecten en las redes de la administración.

2. Mejorar las **capacidades de detección y reacción**. Para ello se deben mejorar o desarrollar **sistemas de alerta temprana** e incrementar la seguridad de los productos y tecnologías desde su fase de diseño. En este sentido, el Sistema de Alerta Temprana del **CCN-CERT**, tanto en la red SARA como con las sondas de Internet instaladas en algunos ministerios y organismos está permitiendo disponer de una visión en tiempo real del estado de la seguridad de las redes monitorizadas, implantar medidas de seguridad adicionales que impidan que ataques similares se vuelvan a reproducir, y detectar patrones de ataques comunes a diversas organizaciones que permiten aplicar de forma eficaz medidas de contención y eliminación de los mismos.

3. Colaborar con la Administración autonómica y local y con el sector privado para apoyar iniciativas que mejoren la seguridad de los sistemas nacionales, haciendo especial énfasis en los que gestionan **infraestructuras críticas**. Extender las acciones de formación y concienciación en ciberseguridad a todos ellos.

4. Concienciar y proporcionar **apoyo a los ciudadanos** para hacer más segura su actividad en línea *(on-line)*, así como reforzar la capacidad de las fuerzas y cuerpos de seguridad del Estado para combatir el cibercrimen.

5. Fortalecer el entorno futuro de ciberseguridad. Para ello se debe incrementar el número de especialistas en seguridad de las TIC, impulsar y coordinar los esfuerzos de investigación y desarrollo de productos de seguridad nacionales, y definir estrategias que disuadan la actividad hostil o dañina en el ciberespacio.

No obstante, para conseguir estos objetivos y como han realizado otras naciones se debe dotar de los recursos precisos a las agencias con misiones en la seguridad de los sistemas TIC de la Administración y a las unidades encargadas del ciberdelito en las Fuerzas y Cuerpos de Seguridad del Estado (FCSE). ■

Javier Candau Romero
Subdirector General Adjunto en funciones
CENTRO CRIPTOLÓGICO NACIONAL
CCN