>> Jorge Dávila

18 meses después

La política interior americana no se ha resentido por el 11-S, más aún, muchas cosas han cambiado en los EEUU desde entonces y algunas de ellas sorprenden. Desde entonces el Presidente Bush y su administración promueven el *e-Government* y la informatización generalizada del Gobierno Federal, la seguridad informática se convierte en un frente estrella en los presupuestos generales del estado y de la investigación académica, surgen campañas públicas a todos los niveles para hacer más seguro el ciberespacio, etc.; sin embargo, en nuestro país parece que no nos hemos enterado todavía.

La ley de 2002 sobre Seguridad Nacional, el denominado "**Homeland Security Act of 2002**", presentada por el presidente de los Estados Unidos como una consecuencia directa de los acontecimientos acaecidos en la ciudad de Nueva York el 11 de septiembre del año 2001, ha visto finalmente la luz en los últimos meses del pasado año[1]. En Estados Unidos, la digestión política de los mencionados actos se plasma en varias iniciativas, pero la más conocida es la creación de un nuevo departamento ejecutivo, la Secretaría de Seguridad Nacional, cuya misión es la de prevenir los ataques terroristas, reducir la vulnerabilidad de los EEUU frente al terrorismo, así como minimizar los daños y ayudar en la reconstrucción después de que un ataque terrorista haya ocurrido.

Las responsabilidades principales de ese nuevo departamento son el análisis de toda la información disponible y la protección de las infraestructuras nacionales, así como el diseño de las contramedidas[2] que sean necesarias. Esta secretaría también se encarga de la seguridad de las fronteras y del transporte, de la disponibilidad y de la respuesta ante ataques terroristas y, por último, de la coordinación, provisión de medios y entrenamiento de otras agencias ejecutivas en estos temas. El secretario de Seguridad Nacional que dirige esta agencia es nombrado directamente por el presidente de los EEUU con el asesoramiento del Senado.

A partir de este nuevo año, esta nueva agencia será la que se dedique a recibir y analizar toda la información acumulada en los servicios de inteligencia y en cualesquiera otras fuentes accesibles, para identificar cuáles son las potenciales amenazas terroristas y entender la naturaleza y extensión de las mismas. Además, esta agencia deberá detectar y asesorar sobre las **vulnerabilidades** presentes en los **recursos clave** y en las **infraestructuras críticas** de los EEUU y, además, deberá desarrollar un **plan nacional de protección**, así como tomar y comprobar la eficiencia de todas las medidas de protección.

Esta secretaría administra todo el sistema de seguridad nacional americano y ostenta la responsabilidad última sobre los anuncios públicos de la amenaza terrorista y proveerá los sistemas de información específicos para su difusión, a la vez que informan sobre las acciones y contramedidas a tomar. Por último, cabe también mencionar que esta agencia es la encargada de revisar, analizar y hacer recomendaciones para la mejora de las **políticas y procedimientos de seguridad** a seguir en temas de inteligencia y cualquier otra información relacionada con la seguridad nacional.

Para tan magna concentración de tareas sensibles y de responsabilidades clave, la administración Bush ha hecho que esta nueva agencia aglutine a otras anteriores, y las funciones que le han sido transferidas son, entre otras, las que antes correspondían al NIPC[3] del FBI incluyendo muchas de las funciones del Fiscal General, las del NCS[4] del Departamento de Defensa junto con algunas de las funciones que tenía en ello el Secretario de Defensa, las funciones de la CIAO[5] del Departamento de Comercio, las funciones del CSD[6] del NIST[7], las del NISAC[8] del Departamento de Energía, y las del FedCIRC[9] de los Servicios Generales de la Administración.

Aunque algunos (no todos) consideran muy serias las amenazas terroristas sobre los sistemas informáticos americanos, en lugar de producirse una recesión o estancamiento, los presupuestos americanos para el año 2003 dedican un total de **50 billones** americanos de dólares de inversión en **Tecnologías de Información** en todos los ámbitos del gobierno federal. Esta enorme inversión en tecnología se presenta, por la administración republicana, como una oportunidad para mejorar los resultados de otros tantos billones americanos de dólares ya asignados/gastados, aumentando la eficacia y la eficiencia de la administración pública americana. La Oficina de Gestión de Presupuestos de la administración americana tiene ya en marcha 21 distintas iniciativas de *e-Government* para aumentar la productividad del gobierno federal mediante su mejora tecnológica, la eliminación de sistemas redundantes, y aumentando significativamente la calidad de los servicios que presta a ciudadanos, empresarios, y a otras administraciones.

El gobierno americano no sólo no frena su informatización, sino que pone los temas de seguridad informática entre los de más interés para el sistema de ciencia y tecnología americanos.

Los presupuestos americanos también recogen un aumento de **722 millones** de dólares para poner en marcha un programa encaminado a utilizar las tecnologías de la información para compartir mas eficientemente la información e inteligencia nacional, tanto horizontalmente (entre agencias) como verticalmente (entre las distintas administraciones). Estas iniciativas de seguridad nacional constituyen un componente clave en la "*expansión de la Administración Electrónica*" que propugna activamente el presidente Bush. Este saneamiento y revitalización dará como resultado un sistema de información sobre los ciudadanos y residentes en los EEUU y al servicio de la policía y el ejército como nunca antes se había visto en la metrópoli de occidente.

El gobierno americano no sólo no frena su informatización, sino que pone los temas de seguridad informática entre los de más interés para el sistema de ciencia y tecnología americanos. La Secretaria de Seguridad Nacional, actuando a través de la Secretaria de Estado de Ciencia y Tecnología, ha sido autorizada para contratar investigaciones específicas financiándolas con fondos federales especiales y, además, para

1 HR5005 - Ley Pública 107-296 de 25 de noviembre de 2002, buscar en http://thomas.loc.gov/
2 Todo tipo de contramedidas: químicas, biológicas, radiológicas, nucleares y relacionadas.
3 NIPC = National Infrastructure Protection Center, www.nipc.gov. Los presupuestos del NIPC para el 2003 son de 125 millones de dólares y sería el primer Centro de Respuesta ante Amenazas Terroristas dentro del FBI. Este presupuesto supone un incremento del 66% respecto al presupuesto del 2002.
4 NCS = National Communications System, www.ncs.gov
5 CIAO = Critical Infrastructure Assurance Office, www.ciao.gov
6 CSD = Computer Security Division, http://csrc.nist.gov/
7 NIST = National Institute of Standards and Technology, www.nist.gov
8 NISAC = National Infrastructure Simulation and Analysis Center
9 FedCIRC = Federal Computer Incident Response Center, www.fedcirc.gov
10 HR5005 Sec. 305 – Federally Funded Research and Development Centers.

desarrollar centros especializados que proporcionen un análisis independiente de los temas de seguridad nacional[10].

La agencia HSARPA

Dentro de esa misma ley[11] americana se pone en marcha la agencia HSARPA[12] para la financiación de proyectos académicos de investigación avanzada en temas de seguridad informática. El director de esta agencia usará sus fondos para permitir y fomentar la investigación básica y aplicada en temas relacionados con la seguridad nacional, para promover cambios revolucionarios en las tecnologías que pudiesen mejorar la seguridad nacional, para avanzar en el desarrollo y evaluación de tecnologías críticas para la seguridad nacional, y para acelerar la construcción de prototipos y el desarrollo de tecnologías que pudiesen poner de manifiesto las vulnerabilidades de la seguridad nacional.

Cyber Security Research and Development Act

En esta misma línea, el 16 de octubre del año pasado aparece el *Cyber Security Research and Development Act*[13] (CSRDA) en el que se reconocen serías deficiencias[14] en los sistemas informáticos y de comunicaciones, y de cómo estos sistemas constituyen la esencia de la realidad americana como nación moderna. Como causas de esa situación se menciona la falta de financiaciones a largo plazo para el desarrollo de tecnologías de seguridad informática, la presencia de una seria descoordinación entre las iniciativas públicas y privadas, la ausencia de suficientes investigadores sobre esos temas, etc. A la vista de ello, el ejecutivo concluye que la inversión federal en esos temas debe aumentarse, concretamente, para mejorar la detección de vulnerabilidades y el desarrollo de sus correspondientes soluciones tecnológicas, para expandir y mejorar la cantera de profesionales de seguridad en las TIs e investigadores del mundo académico, y para coordinar mejor que la información se comparta entre las iniciativas pública y privada. Por ello se concederán becas para la investigación básica e innovadora en las estructuras de las redes de ordenadores, así como para la evolución del hardware y software que las componen.

Las áreas de investigación a fomentar con el CSRDA incluyen, en concreto, **la autenticación**, la **criptografía** y otras tecnologías de **comunicación segura**, las técnicas de **detección de intrusos** y la **informática "forense"**, la robustez de los ordenadores, redes, aplicaciones, sistemas operativos y de control, las infraestructuras de comunicaciones, la **privacidad** y la **confidencialidad**, las arquitecturas de seguridad en redes con herramientas para el análisis y administración de la seguridad, las **amenazas emergentes**, la **detección y reconocimiento de vulnerabilidades**, así como en las **técnicas para cuantificar el riesgo**, la seguridad en acceso remotos y en **sistemas inalámbricos**, etc.

Como los problemas no se resuelven con sólo nombrar unas cuantas comisiones y agencias *ad hoc*, la administración Bush ha decidido que el presupuesto dedicado a ello por la NFS en el quinquenio 2003-07 sea de **233 millones** de dólares para proyectos de investigación, **144 millones** para el desarrollo de centros e infraestructuras específicas, **191 millones** para becas de formación de todo tipo de profesionales e investigadores en temas de "*Computer and Network Security*", y otros **307 millones** de dólares en otras actividades relacionadas, con lo que suma un total no despreciable de **875 millones** de dólares.

En EEUU no sólo no se abandona la idea de informatizarlo todo por miedo a los fallos de seguridad, sino que están convencidos de que esa misma automatización, adecuadamente aderezada con serias iniciativas para fortalecer la seguridad informática, les hará mas fácil defenderse del inevitable terrorismo cibernético.

La Estrategia Nacional para hacer seguro el Ciberespacio

Por si todo esto fuese poco, el pasado 18 de septiembre, Richard Clarke, asesor especial del presidente Bush para temas de seguridad en el ciberespacio, anunció el lanzamiento de una **"Estrategia Nacional para hacer seguro el Ciberespacio"**[15] durante una conferencia en la universidad de Stanford. Esta iniciativa se presenta como un intento para establecer una política nacional y unos principios de guía que permitan proteger el ciberespacio a todos los niveles; desde el mismo usuario doméstico, hasta la protección de sectores nacionales críticos. El borrador, disponible en Internet, contiene un total de 86 recomendaciones, la mayoría de ellas "clásicas y vetustas", que son perfectamente aceptables en cualquier escenario informático e incluso en el de nuestro país. Como nada puede ser perfecto, esta iniciativa americana se anima a dar **"recomendaciones globales"** con las que hay que tener cuidado ya que van mas allá de la soberanía USA y afectan seriamente a la del resto del mundo[16].

En estos casi 18 meses que nos separan del 11-S, la administración americana no se ha quedado quieta y ha seguido tenazmente con su deseo de utilizar la recién estrenada amenaza terrorista como elemento motivador de la actividad productiva de los EEUU. En particular y curiosamente, parece que esto ha favorecido muy seriamente el e-*government* y, por transitividad, a la seguridad informática. No solo no se abandona la idea de informatizarlo todo por miedo a los fallos de seguridad, como muchas veces se argumenta en tertulias conservadoras de nuestro país, sino que los americanos están convencidos de que esa misma automatización, adecuadamente aderezada con serias iniciativas para fortalecer la seguridad informática, les hará mas fácil defenderse del, según ellos, inevitable terrorismo cibernético (afirmación que podría discutirse, pero no lo haremos ahora).

Si dejamos la metrópoli del imperio y nos preguntamos qué ha pasado en ese mismo tiempo en esta parte del mundo, es decir, en la Unión Europea o en nuestro país si queremos concretar más, veremos que nada tiene que ver con el caso americano. El gobierno y la administración española no sólo no han seguido las tendencias de informatización del mundo occidental en el que dicen querer enmarcarse, sino que ha logrado que haya una recesión[17] en el nivel de usuarios. La actual administración española no ha sido capaz de ejecutar apenas el 50% del presupuesto del plan "Info XXI" y el plan "Internet para Todos" sólo ha formado a la décima parte del millón previsto[18].

Está claro que al gobierno español le convendría preguntarle a su amigo americano, en su próxima audiencia, qué es lo que están haciendo en estos temas ya que, de no hacerlo así, nos quedaremos una vez mas como en "Bienvenido Mister Marshal"; viendo pasar un coche negro a toda velocidad. ■

Jorge Dávila Muro
Director
Laboratorio de Criptografía
LSSI – Facultad de Informática – UPM
jdavila@fi.upm.es

---

[11] HR5005 Sec. 307 – Homeland Security Advanced Research Projects Agency. Las responsabilidades de esta agencia son las de administrar sus fondos para poner en marcha un sistema competitivo de financiación, basada en la revisión de méritos y resultados, basado en acuerdos cooperativos o contratos con entidades públicas y privadas, incluyendo empresas, centros públicos de investigación y desarrollo, y universidades.

[12] HSARPA = Homeland Security Advanced Research Projects Agency

[13] HR03394 - Cyber Security Research and Development Act

[14] Un grupo del Departamento de Defensa concluyó ya en 1997 que existía una severa falta de preparación frente a un ataque coordinado físico y cibernético a la infraestructura militar y civil de los EEUU.

[15] NSSC = National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html)

[16] En particular, aquella recomendación que dice "*animar a todas las naciones a aceptar leyes de ciber-seguridad adecuadas* [para los americanos] *de modo que las fuerzas del orden y la justicia americanas puedan investigar y perseguir ciber-crímenes cometidos contra los intereses de los Estados Unidos independientemente de si se originan domésticamente o en el extranjero*"

[17] Ciberpais 19/12/2002: "Internet retrocede en España" | Ciberpais 26/12/2002: "Internet está en recesión en España", asegura el fundador de la primera web | Ciberpais 19/12/2002: "El curso 'Internet para Todos' no llega ni a la décima parte de sus objetivos" | EL PAIS 17/12/2002: "El Gobierno admite que sólo 90.000 alumnos estudian 'Internet para todos' y que no logrará el millón en marzo".

[18] España es un país desarrollado, pero casi el 80% de su población no usa Internet.