

MUCHO TORO

La administración estadounidense las está pasando canutas para atender, con éxito, los deseos de su presidente Barack Obama en materia de lo que allí se denomina ciberseguridad. Pasan y pasan las semanas y no hay manera de que alguno de los candidatos a asumir las funciones de esa figura coordinadora de nueva creación, que es la del denominado *Ciberzar de la Seguridad*, pique el anzuelo y se deje reclutar. Al menos al cierre de esta edición.

¿Por qué tanto rechazo por parte de los sucesivos aspirantes que han ido desfilando y declinando el ofrecimiento –todos ellos profesionales de flamante pedigrí en la materia– a asumir un puesto en principio atractivo y de gran proyección?

Al parecer, los reparos que ensombrecen el ‘goloso’ puesto son principalmente dos: la duda de disponer de una garantía de autoridad suficiente para actuar con autonomía y así poder lidiar con las distintas administraciones con solapadas o fragmentadas competencias en la materia; y el escepticismo de lograr una verdadera interoperabilidad entre dos mundos habitualmente mal avenidos –el público y el privado–, obligados a una imprescindible cooperación en la materia que nos ocupa para obtener las mejores garantías de protección de los sistemas de información federales y las redes e infraestructuras digitales del país.

Así pues, ante un creciente escenario de riesgo, con plausibles incidentes de inimaginable pelaje a la vuelta de la esquina, ¿a quién le apetece ser señalado con el dedo acusador de ‘culpable’ por no haberlo evitado?

Si, pese a la trascendencia del asunto, en los últimos años los sucesivos intentos de conformar una estructura viable, con recursos proporcionales para atenderlo, está resultando un reto colosal, ello no es óbice para que Estados Unidos dé por finalizada su actitud laxa ante el tema y pase a dotarse de nuevos medios y organismos para proteger de incursiones de potencias enemigas y terroristas las citadas redes, sistemas e infraestructuras; y estar en disposición, si procede, de repeler eventuales ataques cibernéticos y, en su caso, perpetrarlos con unidades especializadas.

Todo hace pensar que la ciberseguridad seguirá adquiriendo una relevancia creciente, aunque eso sí, con las consabidas luces y sombras en sus nuevos escenarios de ‘aplicación’. La consideración del ciberespacio como el ‘cuarto campo de batalla’ aboca a la inexorable conformación de estrategias de seguridad digital, por lo que las fronteras entre la ciberdefensa y la ciberguerra se difuminan y al tiempo se contaminan mutuamente. Acaso no sea descabellado pensar que pueda utilizarse el subterfugio de la ciberseguridad como una fachada para la ciberguerra.

Lo que está sucediendo al otro lado del Atlántico debería hacernos reflexionar a los europeos. Hay que aparcar nuestra sempiterna actitud pasiva y no quedarnos como simples espectadores de este drama de alcance planetario. Vienen oportunidades de mover ficha, de construir las cosas como es debido –véase si no el semestre español al frente de la UE en 2010– pero, por favor, apliquémonos el cuento, aprendamos de los errores del vecino y no dilapidemos esfuerzos en iniciativas cojas, dispersas y egoístas. ●



LUIS G. FERNÁNDEZ
Editor
lfernandez@codasic.com