Comentario THIBER:

La necesidad de un programa nacional de ciber-reserva

AUTOR: Guillem Colom, director de THIBER, the cybersecurity think tank

El valor estratégico del ciberespacio está fuera de duda. Paradójicamente, ello contrasta con la escasez crónica de recursos en materia de ciberseguridad, especialmente en el sector público. Es una realidad ampliamente conocida y parece estar asumida por muchos gobiernos, conocedores de la imposibilidad de formar, captar – especialmente en nuestro país debido a la inherente inflexibilidad de nuestra administración pública – y retener el talento en esta materia. Para resolver estas carencias, una de las soluciones propuestas pasa por crear programas nacionales de ciber-reserva. Estados Unidos, Reino Unido, Francia, Estonia o Israel son tan solo algunos de los países que, con enfoques muy diferentes, han puesto en marcha programas experimentales con el objetivo de crear unidades de ciber-reservistas capaces de prestar apoyo a la administración pública y al ámbito militar en caso de crisis o conflicto. Esta realidad es ampliamente analizada por THIBER en su informe "La necesidad de un programa nacional de ciber-reserva"

La situación del ciberespacio nacional requiere desarrollar un programa nacional de ciber-reserva de amplio espectro. Aplicar el ciber-reservismo únicamente a la vertiente tecnológica o militar del ciberespacio sería un grave error estratégico, máxime cuando ha quedado patente que este ámbito afecta a todos los sectores de la sociedad, y que nuestro nivel de madurez se encuentra todavía lejos del mínimo exigible.

Al igual que ocurre en otros países, será necesario contar con un conjunto de expertos – políticos, juristas, intelectuales, comunicadores, grandes empresarios y profesionales TIC de reconocido prestigio – que actúen como **ciber-reservistas estratégicos** con la función de abrir y consolidar este debate político.

En definitiva, es necesario influir en el decisor político sobre esta materia. A día de hoy, la ciberseguridad se encuentra en nuestra agenda política pero no tiene el peso de prioridad política estratégica.

Mientras el gobierno no apruebe un **programa nacional de ciber-concienciación**, es necesario que todos los sectores de la sociedad asuman la importancia estratégica del ciberespacio, así como de su uso seguro y responsable. En la actualidad, las Fuerzas y Cuerpos de Seguridad del Estado, algunos organismos públicos y algunas organizaciones privadas llevan a cabo campañas de concienciación, especialmente dirigidas a estudiantes. A pesar de esta valiosa labor, estas campañas son insuficientes, por lo que será necesario crear una **ciber-reserva ciudadana** que esté compuesta por ciudadanos con la tarea de concienciación sobre la importancia del ciberespacio para la seguridad y desarrollo socio-económico de nuestro país.

A nivel operativo, la escasez de recursos en ciberseguridad hace necesario reclutar a un conjunto de expertos con las habilidades necesarias para prestar apoyo en la seguridad y defensa del ciberespacio nacional. Estos profesionales podrían convertirse en **ciber-reservistas operativos**, tras un exigente proceso de selección, al igual que se hace en otros países. Estos profesionales podrían ser reclutados entre expertos de la administración pública y profesionales del sector privado, recibirían una formación acorde a sus funciones y serían movilizados periódicamente con el fin de integrarlos al sistema nacional de ciberseguridad. Obviamente, no todos los sistemas y servicios podrán incorporar ciber-reservistas, todo dependerá de su nivel de clasificación y criticidad, debiendo prestar estos apoyos no solo a las Fuerzas Armadas sino a todos los organismos civiles con competencias operativas en ciberseguridad. Los miembros de la ciber-reserva operativa deberán realizar programas de capacitación continua, esencial para disponer de una ciberfuerza que permita establecer las medidas de seguridad apropiadas de los ciberespacios que protegen. En cualquier caso, es vital que la capacitación – en caso de que ésta sea necesaria – sea financiada públicamente y no pueda ser objeto de intereses corporativos o individuales, y el compromiso del ciber-reservista reconocido e incentivado.

Es vital que la capacitación – en caso de que ésta sea necesaria – sea financiada públicamente y no pueda ser objeto de intereses corporativos o individuales, y el compromiso del ciber-reservista reconocido e incentivado.

En definitiva, La ciber-reserva debe constituir un elemento importante en la futura revisión de la Estrategia de Ciberseguridad Nacional que, fundamentada en las provisiones de la Estrategia Nacional de Seguridad de 2017, presumiblemente – y quizás dependiendo del calendario electoral – tendrá lugar entre el presente y el próximo año. Pero no debemos olvidar que muchos de nuestros socios y aliados están implementando sus modelos de ciber-reserva como parte integral de una Política de Estado en materia de ciberseguridad, algo que en nuestro país de momento no existe.

Sin embargo, antes de proponer grandes iniciativas que después no serán implementadas con un mínimo de seriedad, serán aplicadas de forma limitada o sin apenas recursos, quizás sería necesario realizar numerosas actividades, desde lograr que la clase política nacional entienda el valor estratégico del ciberespacio y que la construcción de un ciberespacio nacional seguro y resiliente, apoyado por una industria nacional competitiva y no dependiente del exterior debe ser una prioridad. No obstante, como paso previo a la implementación de una ciber-reserva, no sólo sería necesario realizar una intensa labor pedagógica sobre su importancia, sino también generar la confianza suficiente entre todos los *stakeholders* para que este proyecto pueda salir adelante, algo que a fecha de hoy no existe. Igualmente, a nivel político sería necesario realizar un análisis serio y global del estado de riesgo del país, aunque muchas de las amenazas puedan ser comunes cada estado tiene un conjunto de amenazas específicas; diseñar e implementar un modelo de gobernanza racional, donde los diferentes actores con responsabilidad en el ciberespacio nacional trabajen de manera integral, evitando silos y esfuerzos disjuntos; planes de concienciación nacional en materia de ciberseguridad, todos los segmentos de la sociedad civil deben estar concienciados sobre la importancia estratégica del dominio cibernético; fomentar e incentivar el desarrollo de una industria nacional TIC, y en especial de ciberseguridad, si queremos mantener la soberanía nacional en el dominio cibernético; en definitiva, incorporar al ciberespacio en la primera línea de la agenda política nacional e internacional de nuestro gobierno. Todo ello lleva consigo la necesidad de invertir, sin inversión estaremos abocados a la irrelevancia cibernética, cualquier iniciativa que queramos implementar fracasará y pondremos en riesgo no solo el futuro de la soberanía nacional sino también nuestro futuro como sociedad.

“sin inversión estaremos abocados a la irrelevancia cibernética, cualquier iniciativa que queramos implementar fracasará y pondremos en riesgo no solo el futuro de la soberanía nacional sino también nuestro futuro como sociedad.”