THIBER
The cybersecurity think tank

THIBER REPORT Nº1

LA NECESIDAD DE UN PROGRAMA NACIONAL DE CIBER-RESERVA

COPYRIGHT :

THIBER©, the Cybersecurity Think Tank

Todos los derechos reservados. El contenido de esta publicación puede reproducirse o citarse libremente siempre que:

a) Se especifique la autoría del mismo.

b) No se utiliza con fines comerciales ni lucrativos

THIBER no pueden garantizar la ausencia de errores en la publicación.
Una vez detectados, serán modificados en sus sucesivas ediciones.

THIBER REPORTS se publica en Madrid por THIBER, the Cybersecurity think tank

C / Alcalá 75, 2
28009 MADRID
ESPAÑA

Para más información:
www.thiber.org

RESUMEN

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 muy lejos del mínimo exigible para un país avanzado.

ANÁLISIS

Buena parte de los ciudadanos, la mayoría de las empresas y casi la totalidad de los gobiernos del globo son diariamente víctimas de ciberataques con un grado variable de sofisticación e impacto. Sin embargo, lo más preocupante es que, quizás, muchos de estos incidentes pasan completamente desapercibidos debido a la incapacidad de las víctimas para detectarlos. La sustracción de información sensible o el robo de datos de carácter personal, las actividades de espionaje político, militar, económico, industrial o personal, los delitos informáticos con fines económicos o la degradación e inutilización de sistemas militares, industriales, empresariales e infraestructuras críticas son algunos de los objetivos de los ciberataques que acontecen en la actualidad.

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. Este trabajo sigue la estela del comentario que THIBER, the cybersecurity think tank realizó en el Real Instituto Elcano en 2014 y que supuso la primera aproximación a la ciber-reserva en nuestro país.

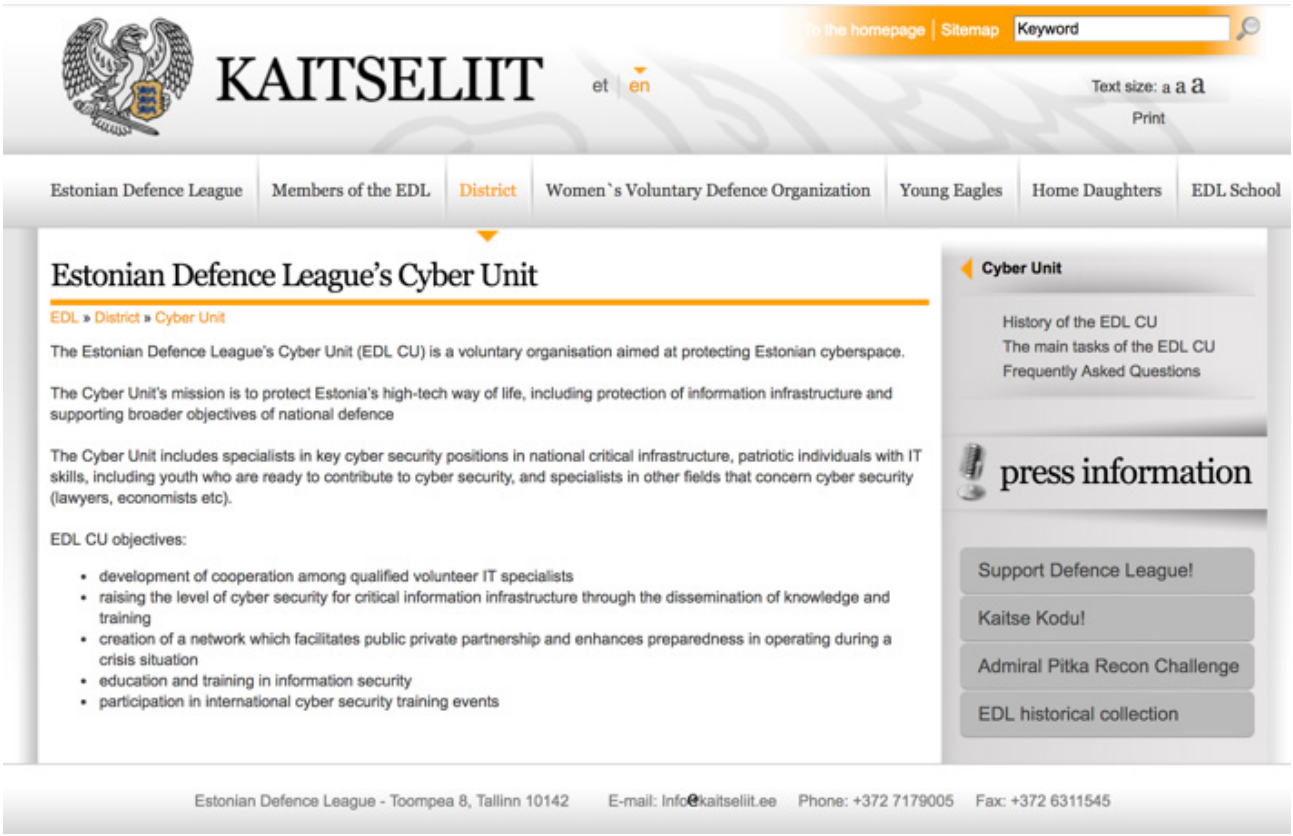
ESTONIA

Estonia, paradigma de nación digital y consciente de la importancia estratégica que posee el ciberespacio para la seguridad nacional desde los sucesos de 2007, hace años que constituyó la Estonian Defence League Cyber Unit. Popularmente conocida como Cyber Defence League (CDL), esta unidad perteneciente a las Fuerzas Armadas cuenta con el apoyo y el soporte del Centro de Respuesta a Incidentes Informáticos del país (Estonian CERT). La CDL está compuesta por un conjunto heterogéneo de profesionales especialistas en ciberseguridad, ciberdefensa y operaciones de información, entre los que se hallan ingenieros, economistas, sociólogos, politólogos, psicólogos o abogados. Su objetivo es prestar apoyo al gobierno en tres puntos esenciales que emanan de la estrategia estonia de ciberseguridad:

- Colaborar en la formación y concienciación de la sociedad estonia sobre el valor del ciberespacio y los efectos que las ciberamenazas pueden tener para este pequeño país.

- Fomentar el crecimiento y madurez de la comunidad de ciberseguridad del país mediante un intercambio efectivo de conocimiento entre sus miembros, pertenecientes éstos al sector público y privado.

- Participar de manera efectiva en la respuesta a cualquier contingencia – incluyendo operaciones de información – que acontezca en el ciberespacio específico estonio.



Página web del Estonian Defence League's Cyber Unit

El relativo éxito de la CDL ha sido posible porque en Estonia concurren un conjunto de circunstancias que no son comunes a todos los países: Estonia es un país pequeño, con una población que no supera los 1,3 millones de habitantes, una administración electrónica bastante madura y con gran dependencia tecnológica. Además, dispone de una administración centralizada en la que cada uno de los actores de su ecosistema cibernético tiene perfectamente definidas sus competencias y actúa de manera integral, sin apenas luchas burocráticas. Las Tecnologías de la Información y las Comunicaciones (TIC), y en especial la ciberseguridad, constituyen uno de los ejes centrales de la agenda política interior (educación, administración, servicios esenciales) y exterior (alianzas e influencia) del gobierno de Tallin, lo que motiva un apoyo gubernamental incondicional a la industria nacional en esta materia, a la que incentiva y apoya, fomentando su expansión e influencia en las naciones de la Unión Europea y la Alianza Atlántica. Finalmente, tampoco puede obviarse el sentido de patriotismo de la sociedad estonia, exacerbado éste tras su independencia de la Unión Soviética y de todos los sucesos que han acontecido desde el final de la Guerra Fría.

"Desde 2016 el Elíseo está trabajando en un modelo de ciber-reserva dual, compuesto por una reserva ciudadana y una operativa."

FRANCIA

Otro caso relevante es el de nuestro país vecino. Francia recientemente publicó la nueva Revi-sión Estratégica de la Ciberdefensa, en la que identifica como una de las máximas prioridades del país la salvaguarda de su soberanía digital. Es por esta razón que la Ley de Programación Militar 2019-2025 ha previsto destinar 1.600 millones de Euros a la "lucha en el dominio ciber-nético". Aunque el grueso del gasto se orientará a la consolidación estratégica de la industria de ciberseguridad y ciberdefensa gala y a la generación de ciberca-pacidades nacionales en esta materia, una parte del presupuesto estará destinado a la remuneración, formación y adiestra-miento de los futuros ciber-reservistas.

En la actualidad, se estima que las Fuerzas Armadas francesas disponen aproximadamente de 3.000 efectivos, con distintos niveles de capacitación cibernética, preparados para lo que el país denomina "combate cibernético", que engloba las funciones de defensa y explotación con las puramente ofensivas. Sin embargo, París estima que esta cantidad es insuficiente y desde 2016 el Elíseo está trabajando en un modelo de ciber-reserva dual compuesto de la siguiente manera:

- Una reserva ciudadana con la misión de generar una cultura nacional de ciberseguridad y ciberdefensa mediante la formación y concienciación de todos los sectores – empresarial, académico o de usuario individual – de la sociedad civil del país.

- Una reserva operativa que, planteada en el Pacto de Defensa Cibernética de 2014, tiene como objetivo asistir al Estado y a las Fuerzas Armadas en caso de que estalle una crisis ci-bernética importante. Sus integrantes colaborarían en la restauración de los sistemas ata-cados bajo la supervisión de especialistas del Ministerio de Defensa, el Ministerio del Inte-rior o la Agencia Nacional de la Seguridad de los Sistemas de Información. Estas agencias también se encargarían de validar su acceso, proporcionar gratuitamente la formación complementaria y garantizar su alistamiento y preparación.

El gobierno pretende que, para 2019, Francia disponga de un cuerpo formado por 4.440 ciber-reservistas organizados de la siguiente forma: 40 miembros permanentes, 400 pertenecientes a la reserva operativa (200 en territorio metropolitano y 200 en el extranjero) y 4.000 pertene-cientes a la reserva ciudadana repartidos por todo el país.

Finalmente, es conveniente subrayar que, a diferencia del caso estonio y de ciertos debates que están surgiendo en nuestro país, el ámbito de actuación de los ciber-reservistas galos no solo se circunscribirá a la defensa de los sistemas informáticos y las redes de comunicaciones del Ministerio de Defensa, sino también podrán proporcionar apoyo táctico a los operadores de infraestructuras críticas civiles, al resto de la administración pública e incluso a sus subcon-tratistas. Además, solamente un grupo reducido de estos ciber-reservistas estaría habilitado para operar en redes clasificadas.

La "réserve de cyberdéfense" francesa

REINO UNIDO

En 2013, el Ministerio de Defensa británico anunció su interés por reclutar a varios centenares de expertos en ciberseguridad con el objetivo de constituir la Reserva Cibernética Conjunta o *Joint Cyber Reserve Force*, vinculada está al *Joint Forces Cyber Group* de las Fuerzas Armadas. Creada para proporcionar una "contribución esencial" a la seguridad nacional del país, esta unidad, eminentemente técnica y circunscrita al ámbito militar, está formada por individuos que abandonan la vida militar, miembros de la reserva activa e incluso sujetos sin experiencia militar previa y selecciona a sus miembros en base a sus conocimientos técnicos, habilidades, experiencia o aptitudes tecnológicas.

Sin embargo, aunque la misma jefatura de estado mayor de las Fuerzas Armadas reconoció que la ciber-reserva debía ser un instrumento eminentemente civil y abrirse a otros ámbitos fuera del estrictamente tecnológico, en la actualidad ésta continúa teniendo una orientación militar y este alcance limitado. Así pues, la función principal de la Reserva Cibernética Conjunta es gestión y captura del talento bajo una óptica de habilidades técnicas y tácticas, sin dar peso a otras habilidades igualmente requeridas en el ámbito de la ciberdefensa, como podrían ser los conocimientos legales, políticos, estratégicos o psicológicos. Además, esta unidad circunscribe su ámbito de actuación a la protección de los activos del Ministerio de Defensa y las Fuerzas Armadas, dándole a la Reserva Cibernética Conjunta un alcance fundamentalmente militar.

Sitio web de la "Joint Cyber Reserve Force" británica

¿SE DAN LAS CIRCUNSTANCIAS EN ESPAÑA PARA PODER IMPLEMENTAR UN PROGRAMA NACIONAL DE CIBER-RESERVA?

A finales de 2013, el gobierno presentó la primera Estrategia de Ciberseguridad Nacional, una estrategia de segundo nivel basada en las provisiones de la Estrategia Nacional de Seguridad que el gobierno popular había presentado en mayo del mismo año. A partir de este momento, el ejecutivo puso en marcha el Consejo de Ciberseguridad Nacional, se comenzó a elaborar tanto el Plan Nacional de Ciberseguridad como los diferentes planes específicos, y se empezaron a articular las acciones encomendadas a los distintos actores con competencias en la materia con el objetivo final de construir un Sistema Nacional de Ciberseguridad.

Sin embargo, la carencia de un presupuesto suficiente y los enormes recursos repartidos de forma más o menos eficiente entre las distintas administraciones públicas, las luchas de poder entre los múltiples actores con competencias en materia de ciberseguridad, una limitada visión estratégica, una planificación más formal que real de las actividades a desarrollar y una alarmante falta de compromiso político han condicionado los desarrollos en esta materia, lastrando indefectiblemente nuestra capacidad presente y nuestra preparación de cara al futuro. En consecuencia, antes de plantear un programa de ciber-reserva que reproduzca uno de los distintos modelos externos, pero sin adaptarse a la idiosincrasia y características propias de nuestro país, que genere desconfianzas entre sus potenciales integrantes porque obvia sus demandas, que no obtenga un amplio respaldo político y social necesario para su eficaz implementación, que pueda circunscribirse únicamente al Ministerio de Defensa obviando la dimensión estratégica del dominio cibernético o que pueda utilizarse para resolver carencias estructurales en esta materia, antes será necesario realizar un diagnóstico de la situación y observar de qué capacidades se dispone, cuáles son las carencias identificadas, qué medios pretenden utilizarse y cómo se integraría en el esquema de seguridad nacional.

ANÁLISIS DE LA SITUACIÓN ACTUAL

Sin ánimo de ser exhaustivos, ya que el objetivo de este breve documento es la generación de ideas para apoyar al necesario debate público sobre la ciber-reserva nacional, a continuación se plantearán a grandes rasgos algunos de los condicionantes que a día de hoy existen en esta materia y que, quizás, requerirían ser resueltos antes de proceder al diseño de una ciber-reserva nacional.

En primer lugar, formalmente todos los actores del sistema nacional de ciberseguridad tienen unas responsabilidades claras y unas competencias concretas, reguladas (aunque en muchos casos con normas que requerirían ser armonizadas y actualizadas) y supervisadas, lideradas y coordinadas por el Consejo Nacional de Ciberseguridad. Por lo tanto, se asume que cada uno de ellos diseña sus capacidades atendiendo a las funciones que tiene encomendadas, las desarrolla de forma autónoma teniendo en cuenta su armonización con el resto de los actores

y las pone en común para así dar forma y garantizar la operatividad del Sistema Nacional de Ciberseguridad. Aunque la publicación de la Estrategia de Ciberseguridad Nacional en 2013 representó un hito en esta materia y ha permitido avanzar en la construcción de una arquitectura y un sistema de gobernanza del ciberespacio nacional, también es cierto que este sistema se ha desvirtuado: algunos actores han adoptado posturas de *free rider* para intentar asumir responsabilidades y funciones que no les corresponden, no ha existido una coordinación lo suficientemente efectiva para armonizar en lo posible el desarrollo de capacidades y homogeneizar el nivel de madurez cibernética de los distintos actores y el sistema de gobernanza propuesto, encabezado por el Consejo Nacional de Ciberseguridad, se ha demostrado poco operativo. Problemas similares también ocurren entre la Administración General del Estado y otras administraciones autonómicas, por lo que el desarrollo de capacidades es menos homogéneo, efectivo y más compartimentado de lo que cabría esperar.

"No puede pretenderse que la ciber-reserva se encuadre en el ámbito del Ministerio de Defensa ni las Fuerzas Armadas tal y como sucede con la Reserva Voluntaria, cuya efectividad es más formal que real y el apoyo recibido por ha sido más bien escaso."

<u>En segundo lugar,</u> aunque la Estrategia de Ciberseguridad Nacional realiza un diagnóstico de los principales riesgos y amenazas que se ciernen sobre el ciberespacio global y nacional, este estudio no sólo debería ser actualizado – algo previsible tras la publicación de la nueva Estrategia de Seguridad Nacional de 2017 – para dar cuenta de los avances en esta materia, sino también ampliado. En este sentido, es esencial disponer de un documento actualizado, detallado y dinámico que identifique las tendencias presentes y futuras en materia de riesgos y amenazas, el estado de riesgo nacional, la madurez, capacidades y resiliencia de nuestro ciberespacio específico, cuáles son los activos estratégicos que deben ser defendidos y cuáles son los medios a utilizar y las capacidades a madurar para el logro de estos objetivos. En otras palabras, la futura Estrategia de Ciberseguridad Nacional debería establecer los fines *(ends),* modos *(ways)* y medios *(means)* para la construcción de un ciberespacio nacional seguro y resiliente, siendo la ciber-reserva una parte integral de este ecosistema. De la misma manera, las líneas de acción planteadas en la Estrategia de Ciberseguridad Nacional para construir el sistema nacional de seguridad no sólo deberían trazarse con más detalle y fijar acciones específicas para que cada uno de los actores aumentara sus capacidades; sino muy especialmente incrementar y racionalizar la dotación presupuestaria (algo que quizás requeriría con carácter previo realizar un estudio sobre el gasto en materia ciber en las distintas administraciones), reducir la compartimentación de las competencias y establecer métricas para evaluar el progreso en el desarrollo de capacidades.

En tercer lugar, otro elemento a tener en cuenta antes de proceder a la creación de la reserva sería la dependencia orgánica de ésta. No puede pretenderse que ésta se encuadre en el ámbito del Ministerio de Defensa ni las Fuerzas Armadas tal y como sucede con la Reserva Voluntaria, cuya efectividad es más formal que real y el apoyo recibido por parte del Ministerio de Defensa ha sido más bien escaso. Una reserva estratégica que pueda ser utilizada para una amplia gama de cometidos ni debe tener carácter militarizado ni tampoco depender de uno de los actores del esquema nacional de ciberseguridad. Planteada en el marco de un Enfoque Integral a la seguridad nacional, esta capacidad debería tener una dependencia directa del Departamento de Seguridad Nacional, puesto que éste se constituye como el máximo órgano en materia de coordinación de la seguridad de nuestro país.

"el programa nacional de ciber-reserva debería ser un programa planificado, dinámico y con dotación presupuestaria que, a corto plazo, debería enfocarse a la consecución de tres objetivos: influencia, concienciación y operación."

Si se encauzan estos problemas organizativos y se logra una radiografía suficientemente clara sobre la situación particular de nuestro ciberespacio específico, será posible plantear un modelo de ciber-reserva adecuado a nuestras necesidades específicas. No obstante, quedarán pendientes todavía otros asuntos de vital importancia y que pueden decidir el éxito o fracaso de esta iniciativa, tal y como puede ser la generación de una comunidad de confianza, que a fecha de hoy es muy limitada, entre los proponentes de la reserva y muchos de sus posibles integrantes.

HACIA UN PROGRAMA NACIONAL DE CIBER-RESERVA

No cabe duda de que el programa nacional de ciber-reserva debería ser un programa planificado, dinámico y con dotación presupuestaria que, a corto plazo, debería enfocarse a la consecución de tres objetivos: influencia, concienciación y operación. En este sentido, el programa podría articularse en tres ramas: ciber-reserva estratégica, ciber-reserva ciudadana y ciber-reserva operativa. A continuación se explicarán brevemente sus posibles características:

La Estrategia de Ciberseguridad Nacional ha supuesto un hito importante pero ha fracasado en uno de sus objetivos más ambiciosos: crear una **cultura nacional de ciberseguridad.** Sigue siendo necesario y urgente, abrir un debate político sobre aspectos fundamentales como legislación, industria nacional de ciberseguridad, I+D+i en materia de ciberseguridad, concienciación y formación sobre los riesgos y amenazas en este ámbito. Al igual que ocurre en otros países, será necesario contar con un conjunto de expertos – políticos, juristas, intelectuales, comunicadores, grandes em-

presarios 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 profesionales 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.

CONCLUSIÓN

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, hasta conseguir que la opinión pública entienda que lo ciber está en su vida diaria. 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.

THIBER

The cybersecurity think tank

Follow us:
www.thiber.org