A LA MESA DEL SENADO

El **GRUPO PARLAMENTARIO POPULAR**, al amparo de lo establecido en los artículos 174 y 175 del Reglamento de la Cámara, tiene el honor de presentar la siguiente **MOCIÓN**, para su debate en el Pleno de la Cámara.

Uno de los problemas más complejos a los que nos estamos enfrentando y nos deberemos enfrentar en el futuro, son las nuevas formas de delinquir a través de la red y que afectan tanto al sector público como privado. Los conocidos como ciberataques están generando múltiples problemas en todo los países. Unos son amparados por Estados que los perpetran ellos mismos o pagan a alguien para que los realice, otros son apadrinados por sociedades mercantiles y por organizaciones criminales o terroristas, pero en todos los casos , sus víctimas son tanto los sectores públicos como privados, así como la sociedad civil y la ciudadanía.

La seguridad al ciento por ciento no existe en el ciberespacio, pero todos los expertos concluyen que sí se pueden minimizar los riesgos de ataques de esta naturaleza y en el caso de que se materialicen mitigar los impactos para recuperar la normalidad.

Por este motivo llama la atención que encuestas realizadas a un considerable número de directivos en España en relación al nivel de protección de las empresas ante este tipo de ataques, han concluido que queda mucho por hacer. En este sentido, el 67,7% de los directivos encuestados consideran que sus empresas tienen una alta probabilidad de sufrir este tipo de delincuencia, y el 49% reconocen que carecen de una estrategia integral de seguridad. El 53% dice no contar con programas de formación para sus empleados.

El problema no está sólo en lo que sucede en un ordenador, si no en el efecto multiplicador que tiene Internet y su capacidad para amplificar el daño. El carácter asimétrico del ciberespacio, su capacidad de anonimato y la dificultad de las investigaciones y persecución de los ciberataques hacen aún más complicado el contexto. Además, todo se dificulta desde el momento en que las distintas organizaciones van integrando un mayor número de dispositivos y elementos que se conectan entre sí.

Los riesgos aparecen simplemente por ser clientes o usuarios de cientos de servicios digitales y formar parte del entramado digital del

ciberespacio con nuestras conexiones a Internet, el correo electrónico, las redes sociales, los smartphones, tablets, smartwatchs, etc. Por ello, hemos pasado a ser víctimas y objetivos de los ataques y, en muchos casos, incluso miembros involuntarios de un ejército en manos desconocidas. Es muy fácil, una vez se tiene las herramientas y maquinaria suficiente, operar a gran escala, a través de redes de ordenadores y dispositivos comprometidos y controlados por ciberdelincuentes.

Además, otro elemento a tener en cuenta es la utilización del ciberespacio en la denominada Guerra Híbrida, que mediante la combinación de diferentes tácticas busca desestabilizar y polarizar la sociedad de los estados evitando el conflicto armado, pero a la vez consiguiendo que dichas acciones aparezcan como deliberadamente ambiguas.

En los últimos meses han aparecido noticias preocupantes relacionadas con la Ciberseguridad. Desde cómo se ha intentado influir en procesos electorales en países de nuestro entorno, incluyendo los últimos acontecimientos en Cataluña, intentando desestabilizar nuestro régimen de libertades, así como los ataques sufridos por algunas multinacionales como es el caso de SONY y el caso de los virus o malwares Wannacry o Petya, que afectó a grandes empresas de todo el mundo y cuyos objetivos eran conseguir un rescate a cambio de recuperar los archivos bloqueados, poner en jaque la disponibilidad de servicios esenciales, pudiendo afectar a infraestructuras gubernamentales o la estabilidad de un país, y extenderse por la Red buscando otras víctimas.

Entendemos que al Gobierno le toca jugar, y debe jugar un papel primordial en este terreno de la Ciberseguridad, dado que es un ámbito de especial interés para la seguridad nacional, tal y como recoge la Ley 36/2015 de Seguridad Nacional.

El Ciberespacio es un dominio muy complejo, y por tanto, uno de los principales roles que debe adoptar es el de impulsar el crecimiento y la protección en materia de Ciberseguridad.

Para ello, dispone de múltiples organismos. En el nivel estratégico político el Consejo Nacional de Ciberseguridad y Departamento de Seguridad Nacional como Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y con un papel de relevancia en la gestión de crisis en este ámbito, distintos Ministerios con competencias concretas en este ámbito a través de organismos que actúan en el nivel operacional como son: el Instituto Nacional de Ciberseguridad-INCIBE (anterior INTECO), el Centro Nacional para la Protección de las

Infraestructuras y Ciberseguridad (denominación actual) Críticas (CNPIC), el Centro Criptológico Nacional (CCN),) y, en el ámbito de la defensa a nivel militar, el Mando Conjunto de Ciberdefensa. Asimismo también se cuenta con documentos estratégicos que orientan la acción en esta materia como es la Estrategia Nacional de Ciberseguridad, el Plan Nacional de Ciberseguridad y nueve planes derivados que responden a las líneas de acción de la Estrategia Nacional de Ciberseguridad a través de acciones concretas o la aprobación del Esquema Nacional de Seguridad (ENS).

Por otra parte sin duda es necesario seguir avanzando en la colaboración público privado y en esta línea estamos de acuerdo con los puntos expuestos en la moción.

Por todo cuanto antecede, el **GRUPO PARLAMENTARIO POPULAR** propone a la aprobación del Pleno del Senado la siguiente:

MOCIÓN

El Senado insta al Gobierno a continuar definiendo las prioridades y los objetivos de protección en materia de Ciberseguridad colaborando en la puesta en marcha de planes de apoyo que mejoren la colaboración público-privada en esta materia, y para ello deberá continuar trabajando en:

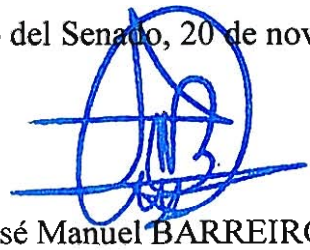
1.- Impulsar canales de cooperación entre lo público y privado.

2.- Tener agilidad para adaptarse y responder a las distintas amenazas.

3.- Conocer y dar respuesta a las demandas de los actores del mundo ciber.

4.- Desarrollar una actitud proactiva de comunicación y de coordinación y no solo reactiva tras un incidente.

Palacio del Senado, 20 de noviembre de 2017.



José Manuel BARREIRO FERNÁNDEZ
PORTAVOZ

/PD