INFORME DE ESPAÑA SOBRE CUMPLIMIENTO DE RESOLUCION 68/243

En cumplimiento del párrafo 3 de la Resolución AG 68/243 sobre Los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, a continuación se remite la posición de España sobre las cuatro cuestiones requeridas:

a) Visión sobre el tema de la seguridad de la información.

Las nuevas tecnologías de la información y de las telecomunicaciones contribuyen de manera extraordinaria al crecimiento económico y al desarrollo. Por ello, resulta esencial responder a los retos y amenazas que su uso ilícito, delictivo o con fines terroristas plantea a la seguridad de los países y a los derechos fundamentales de las personas.

España considera que los gobiernos deben de apoyar y mantener un ciberespacio abierto, accesible y seguro, salvaguardando al mismo tiempo valores fundamentales como la democracia, los derechos humanos y el estado de derecho.

Es esencial que los países refuercen sus capacidades para estar preparados a la hora de prevenir, detectar y dar respuesta a los riesgos y amenazadas del ciberespacio.

Asimismo, se considera que la cooperación internacional es esencial y que los Estados deben intensificar sus esfuerzos para intercambiar información y buenas prácticas con el fin de apoyar el desarrollo de capacidades en los países que lo necesiten así como adoptar medidas de fomento de la confianza para evitar conflictos y tensiones.

b) Medidas adoptadas en el ámbito nacional y cooperación internacional.

En el plano nacional:

La ciberseguridad se ha convertido en una prioridad estratégica para España, con vistas al desarrollo de la sociedad digital y a garantizar un ciberespacio libre y seguro.

Desde 1992, España ha venido desarrollando una amplia **legislación y normativa** que incide en la seguridad de la información y en la protección del libre ejercicio de los derechos y libertades reconocidos en la Declaración Universal de los Derechos Humanos y en la Constitución española. Abarca tanto normas nacionales como directivas procedentes de la Unión Europea. Una relación de las medidas adoptadas por España en este ámbito puede encontrarse en la **Respuesta de España** contenida en el Informe del Secretario General sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, del 16 de julio de 2013 (A/68/156).

España ha incrementado sus esfuerzos en este campo en particular desde el año 2007, en que se creó el primer **CERT gubernamental** que soporta la capacidad de respuesta a emergencias cibernéticas. Dicho CERT se halla vinculado al **Centro Criptográfico Nacional** y

contribuye diariamente y de forma decisiva a la prevención y lucha contra los ataques cibernéticos.

España ha venido desarrollando, en particular, sus capacidades en materia de Protección de Infraestructuras Críticas que representan una parte fundamental de la seguridad nacional. Para ello, cuenta con la orientación del **Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)**, creado también en 2007, que ha desarrollado una regulación y una metodología propias para la evaluación de este tipo de infraestructuras.

Dicho Centro viene impulsando, además, la colaboración entre los distintos actores con responsabilidad en la materia, a través de los denominados **Partenariados Público-Privados (PPP)**, habiendo desarrollado un **modelo alternativo en materia de regulación del espacio cibernético**. Frente a las dos tendencias encontradas que se han venido identificando en los últimos años en el plano internacional –"modelo de actuación voluntaria" versus "modelo regulatorio"-, la experiencia española presenta un **modelo mixto** que reconoce la conveniencia de introducir cierta regulación al tiempo que persigue sus objetivos mediante incentivos que eviten situaciones de falta de cooperación (y no mediante sanciones).

El modelo mixto combina además la regulación normativa, con el concepto de **Seguridad integral** y la alianza entre actores clave, como es el caso de los Ministerios de Interior y de Industria y Energía. A partir precisamente de esa colaboración entre ambos Departamentos ministeriales, se han conseguido desarrollar capacidades para la constitución de un CERT que da servicio a la totalidad del sector privado español y a la Protección de Infraestructuras Críticas. Este **CERT de Seguridad e Industria** ofrece como novedad la posibilidad de establecer un punto de contacto directo entre los distintos CERT nacionales y las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado, ofreciendo resultados muy satisfactorios.

España destaca además por sus capacidades en materia de lucha contra el Ciberterrorismo y la Cibercriminalidad, habiendo creado una **Fiscalía especializada en materia de Ciberdelito**. Asimismo, promueve la investigación y desarrollo (I+D), las áreas de prevención y concienciación, así como las de preparación y respuesta.

La **Estrategia de Ciberseguridad Nacional,** aprobada el 5 de diciembre de 2013, esta en línea con los objetivos y principios de la Estrategia de Ciberseguridad de la Unión Europea y establece un enfoque integral de la ciberseguridad, fomentando el intercambio de información, con el fin de mejorar el conocimiento sobre amenazas y vulnerabilidades.

La Estrategia de Ciberseguridad Nacional 2013 establece ademas un sistema de coordinación interna para articular y gestionar la respuesta a los ciberataques, en torno al mencionado CERT nacional, y prevé la creación de un **Consejo Nacional de Ciberseguridad**, en el que están representados todos los órganos y departamentos ministeriales con competencias en ciberseguridad.

La Estrategia prevé asimismo un impulso de la colaboración internacional y la necesaria implicación de organismos y empresas, particularmente de aquellas cuya actividad se considera estratégica o crítica. Se incluye, como elemento esencial, la sensibilización de los ciudadanos, profesionales y empresas, acerca de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías, desarrollando programas específicos de educación y concienciación en ciberseguridad.

La Estrategia se desarrollará mediante un Plan Nacional de Ciberseguridad y Planes Derivados para cada línea de acción estratégica.

<u>Cooperación internacional</u>:

España considera muy importante que Naciones Unidas tenga un papel relevante en el proceso tendente a alcanzar un consenso internacional sobre este tema **y d**efiende el desarrollo de un debate institucionalizado en NNUU que favorezca la participación de los Estados y contribuya a la cooperación internacional, permitiendo el establecimiento de estándares globales, mejores prácticas y una regulación internacional que garantice la paz y seguridad en el uso de las tecnologías de la información.

Con ese objetivo, España organizó el 21 de marzo de 2014 en Madrid una **Reunión sobre Ciberseguridad, a nivel de Representantes Permanentes**, y ha elaborado un documento con Conclusiones, que contribuye a enriquecer y profundizar en el debate sobre estas cuestiones. España está dispuesta a seguir trabajando sobre estas cuestiones con otros Estados interesados en el marco de las Naciones Unidas.

España ha sido invitada a designar un Experto para participar en el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, para el mandato 2014-2015, y está comprometida a contribuir activamente con un enfoque pragmático, abierto e integrador.

España participa además activamente en diversas **iniciativas internacionales sobre Ciberseguridad** y promueve una cooperación internacional policial y judicial proactiva en la lucha contra el Ciberterrorismo y Cibercriminalidad, entre otros aspectos. Es parte de la Convención sobre el Ciberdelito, conocida como Convención de Budapest, negociada en el marco del Consejo de Europa, y ha participado activamente en otros foros como la OSCE, la OTAN, UNODC, el Consejo de Derechos Humanos y las Conferencias Meridian en materia de Protección de Infraestructuras Críticas de la Información. Por su destacada labor en este campo se ha propuesto a España que organice la edición de 2015 de las Conferencias Meridian, propuesta que ha sido aceptada.

c) **Conceptos párrafo 2**

Como se ha mencionado en el punto anterior, España defiende el desarrollo de un debate institucionalizado en NNUU y en otros organismos internacionales que favorezca la cooperación internacional y el establecimiento de estándares globales, mejoras prácticas, normas de conducta entre Estados y medidas de fomento de la confianza, con el objetivo último de garantizar la paz y la seguridad en el uso de las tecnologías de la información.

España apoya las recomendaciones del Informe del Grupo de Expertos Gubernamentales de Naciones Unidas de 2013, relativas al diálogo entre Estados para el establecimiento de medidas de fomento de la confianza, el apoyo a la construcción de capacidades en ciberseguridad en aquellos países que lo necesiten, las iniciativas regionales y la aplicación del Derecho Internacional en el ciberespacio.

A este respecto, España considera que es necesario reflexionar sobre cómo las normas y principios de derecho internacional deben aplicarse al comportamiento de los Estados en el uso de las TICs. España considera que siendo ésta una cuestión de gran trascendencia, convendría que fuera abordada en el marco del nuevo Grupo de Expertos Gubernamentales.

.

d) Posibles medidas a adoptar por la comunidad internacional.

España considera que la comunidad internacional debe adoptar medidas en 4 ámbitos de actuación para reforzar la seguridad de la información a nivel global:

1) Medidas de fomento de la confianza:

- Estas medidas se deben adoptar tanto en el ámbito de organismos internacionales y regionales como de manera bilateral entre Estados.
- Las medidas de fomento de la confianza deben incluir intercambio de información sobre Estrategias nacionales, mejoras prácticas e información sobre incidentes y amenazas o creación de puntos de contacto nacionales.

2) Derecho Internacional:

- La comunidad internacional y especialmente Naciones Unidas deben seguir reflexionando sobre cómo se deben interpretar y aplicar los principios y normas del derecho internacional en el ciberespacio, especialmente las relativas a uso de la fuerza, al derecho humanitario bélico y a la protección de los derechos humanos

3) Cooperación internacional:

- Se debe promover la cooperación internacional para hacer frente a las amenazas y riesgos en el ciberespacio, mejorando los canales de comunicación, estableciendo mecanismos de coordinación de CERTs, realizando ejercicios conjuntos, etc.
- Se deben promover y agilizar los mecanismos de cooperación judicial y policial para prevenir y perseguir los crímenes cometidos en el ciberespacio con rapidez y eficacia.

4) Construcción de capacidades:

- Se debe promover la construcción de capacidades en los países que lo necesiten, tanto bilateralmente como en el marco de organismos internacionales, preferentemente de carácter regional.