MIGUEL ÁNGEL BALLESTEROS MARTÍN

"El ciberespacio lleva años consolidándose como un entorno de alta relevancia económica y social, pero también de inseguridad"

Las amenazas a la seguridad de las sociedades occidentales han ido modificándose, adoptando nuevas formas con el paso de los años, en particular desde la caída del muro de Berlín en 1989 y los ataques a las torres gemelas de Nueva York en 2001. ¿Puede vislumbrarse una raíz común en esta hiedra que nos ataca o por el contrario son fenómenos cuyo único elemento común es la amenaza que ejercen sobre nuestra vida cotidiana?, ¿tienen una raíz común o es una miríada de actuaciones con motivaciones diferentes?

Las amenazas se adaptan a las circunstancias del momento y tanto los actores estatales como los no estatales saben aprovechar todo lo que la tecnología ofrece, sin que se sometan a legalidad alguna. Su único criterio es alcanzar su objetivo.

Su labor es más fácil que la de los que nos dedicamos a defendernos. La seguridad tiene que tratar de hacer frente a múltiples ataques posibles, y ellos focalizan sus esfuerzos en un punto donde aplicar toda la contundencia.

La aparición de un nuevo ámbito de actuación global como es el ciberespacio, su débil regulación, las dificultades para realizar atribuciones de autoría que evitan la represalia, y el bajo coste de las acciones, ha propiciado que cada año se incremente el número de ciberataques al tejido empresarial, a las infraestructuras críticas, a los servicios del Estado e incluso a los ciudadanos.

En los últimos años, ¿ha crecido el número de ciberataques? ¿Qué impacto pueden tener en el marco de la seguridad nacional?

El mundo digital crece y por tanto nuestra exposición a los ciberataques también. Los datos de ciberataques de los últimos años nos indican que cada vez se detectan más y, lo más preocupante, cada día son más graves. Particularmente, son especialmente relevantes aquellos que afectan a la economía o a los servicios esenciales

También son frecuentes las acciones en el ciberespacio con la finalidad de debilitar a los países aprovechando la dificultad para atribuir la autoría a un Estado concreto, ya que, con frecuencia, estas acciones se realizan a través de intermediarios o proxis. Eso hace que los ciberataques y las campañas de desinformación sean cada vez más frecuentes en la denominada zona gris de los conflictos, donde la violencia no llega a aparecer. Esto inutiliza la tradicional estrategia de la disuasión por la represalia y dificulta la prevención de los ciberataques.

¿Es el Ciberespacio un ámbito de confrontación entre potencias?

El ciberespacio lleva años consolidándose como un entorno de alta relevancia económica y social, pero también de inseguridad. Un ámbito propicio para la alta velocidad de cambio, donde los riesgos y amenazas son cambiantes, poliédricos, difíciles de evaluar y de predecir.

El enfrentamiento geopolítico en busca de la hegemonía económica, tecnológica e incluso militar ha visto en el ciberespacio un ámbito idóneo como medio. Inevitablemente, potencias como España se ven afectadas por esta confrontación geopolítica.

La confrontación geopolítica en el ciberespacio entre China y EE.UU. es sobre todo por el dominio tecnológico, mientras que Rusia, utilizar el ciberespacio como un instrumento clave en sus estrategias hibridas.

Dentro de las amenazas a la seguridad, las que provienen del mundo digital tienen una particularidad técnica que obliga a contrarrestar los ciberriesgos de manera muy específica en relación al resto de riesgos de seguridad. ¿Estamos preparados en España para esta nueva situación?

La Estrategia de Seguridad Nacional de 2017, considera que una de las dinámicas de transformación global es el ritmo acelerado de transformación, basada en la tecnología que está potenciando la interconectividad en detrimento de la seguridad. Se está empezando el despliegue de las redes 5G que va a suponer un cambio del paradigma del uso del ciberespacio con el Internet de las Cosas o la Industria 4.0 pero que también conlleva importantes riesgos para los intereses de Seguridad Nacional. La correcta gestión de los datos y de la información requieren importantes inversiones en seguridad.

En 2019 se aprobó una nueva Estrategia Nacional de Ciberseguridad (ENCS) que establece cinco objetivos y siete líneas de acción desglosadas en 65 medidas para alcanzarlos. Cada año se realiza un informe para determinar el grado de consecución.

Queda mucho camino por recorrer y muchos retos que abordar. Sin embargo, España ha avanzado considerablemente en la madurez de su Sistema de Ciberseguridad Nacional hasta el punto de que el Global Cybersecurity Index (GCI) elaborado por la Unión Internacional de Telecomunicaciones de Naciones Unidas posiciona a España en el puesto 7º a nivel mundial sólo superada por Reino Unido, EE.UU., Francia, Lituania, Estonia y Singapur. Dicho estudio examina cinco pilares (legal, técnico, organizativo, desarrollo de capacidades y cooperación)

También la Comisión Europea destaca la Estrategia de ciberseguridad de España en el Índice de la Economía y la Sociedad Digitales (DESI) 2020.

> El enfrentamiento geopolítico en busca de la hegemonía económica, tecnológica e incluso militar ha visto en el ciberespacio un ámbito idóneo como medio

¿En qué medida el Foro Nacional de Ciberseguridad que presides es una nueva manera de afrontar los ciberriesgos?

La puesta en marcha del **Foro Nacional de Ciberseguridad**, que es una de las medidas contempladas en

la ENCS, se constituyó el 22 de julio de 2020, como parte del sistema de ciberseguridad nacional. Se trata de un órgano de colaboración público-privada inédito y que está llamado a ser un modelo a implementar en otros ámbitos de la Seguridad Nacional.

El foro ha puesto en marcha tres iniciativas para las que se han creado tres grupos de expertos que están trabajando en los siguientes temas: Cómo reforzar la formación, la educación y cualificación de los profesionales de ciberseguridad; otro grupo que se ocupa de impulsar y apoyar a la industria e I+D+i y la retención del talento; y, por último, un grupo que estudia cómo fomentar la cultura de ciberseguridad, cuyo trabajo se alineará con el Plan Integral de Cultura de Seguridad Nacional.

Los riesgos lo son de carácter global, y los ciberriesgos no escapan a esa premisa. ¿De qué manera se produce la necesaria coordinación en occidente para afrontar los ciberriesgos?, ¿y en Europa de manera más específica?

En este clima de confrontación geopolítica en el ciberespacio, la UE debe jugar un papel relevante y para ello, la clave es actuar lo más cohesionados posibles y apoyar a las empresas europeas que contribuyen al desarrollo del ciberespacio, ya sea como operadores de redes, proveedores, desarrolladores de aplicaciones, empresas de ciberseguridad, etc. La colaboración público-privada nunca fue tan necesaria como ahora.

> La tecnología ha empoderado al ciudadano como centro de las iniciativas y medidas en el campo de la ciberseguridad e involucrando en todo el proceso al sector privado y a la sociedad en un papel de corresponsabilidad

La UE se ha ido dotando de estructuras y normativas para fomentar la ciberseguridad en su territorio. Ya dispone de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) con sede en Atenas, que se ha visto reforzada con la Ley de Ciberseguridad Europea (Cybersecurity Act) sin olvidar una amplia normativa que va desde la Directiva NIS que establece medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, hasta la recientemente aprobada Estrategia de Ciberseguridad de la UE, pasando por la creación de un marco para la certificación de productos, servicios y procesos que pretende aumentar la soberanía digital y la seguridad de Europa o la llamada "Caja de herramientas 5G", que contiene una serie de recomendaciones para la seguridad de las redes 5G. Sin embargo, es mucho el camino que queda por recorrer para alcanzar una mayor cooperación y coordinación en el ámbito de la ciberseguridad.

Para reforzar la ciberseguridad también es fundamental focalizarse en la prevención, por lo que son importantes los ejercicios que se organizan en el seno de la UE y que nos ayudan a fomentar la colaboración entre países y la UE. Uno de esos ejercicios es el Blue Olex que se realiza cada año para aprender a gestionar crisis de ciberseguridad o los Cyber Europe, organizados por la ENISA y a nivel más técnico, acciones todas ellas que nos ayudan a prepararnos antes grandes ciberataques o crisis.

Los 27 Estados miembros de la UE han firmado una declaración conjunta titulada 'Construyendo la nube de próxima generación, para empresas y el sector público en la UE. En ella, acuerdan trabajar juntos para desplegar la infraestructura y servicios de procesamiento de los datos confiables que requieren las administraciones públicas, las empresas y la ciudadanía.

Podemos defendernos de los ciberriesgos, pero ¿cabe adoptar actuaciones proactivas que reduzcan su frecuencia e impacto?

La estrategia apunta que la tecnología ha empoderado al ciudadano como centro de las iniciativas y medidas en el campo de la ciberseguridad e involucrando en todo el proceso al sector privado y a la sociedad en un papel de corresponsabilidad.

Aunque cada año aumenta el número de ciberincidentes, también es verdad que cada año es mayor nuestra capacidad de prevención, detección y respuesta, pero es necesario seguir mejorando nuestras capacidades humanas, materiales, organizativas y de procedimientos. Uno de los mayores desafíos es disponer de personal formado, y de herramientas que permitan la detección temprana, la definición de perfiles de ataques que nos ayuden a identificar las tácticas, técnicas y procedimientos y cada vez más origen para combatirlos con la máxima rapidez. Estas capacidades se complementan con otras preventivas.

Debemos ser cada día más proactivos, en el entendimiento de que la mejor gestión de ciberincidentes es que no ocurran, para evitar la debilidad del que solo reacciona arrastrado por los acontecimientos e iniciativas de los ciberatacantes.

Siempre acabamos las entrevistas con una pregunta doble. ¿Cuál es el mayor riesgo para España en el corto plazo y en el largo plazo? ¿Qué consejo nos ofreces para un joven actuario que se inicie en la profesión?

El DSN todos los años publica un informe de Seguridad Nacional en el que también se hace un análisis de riesgos para los próximos años. Este estudio es el fruto de una encuesta realizada a expertos en los diversos ámbitos de la seguridad Nacional.

En el Informe de 2020, el mayor riesgo que aparece son las epidemias y pandemias por su alto impacto en otros campos como son la economía o la estabilidad social. Es evidente que nadie puede sustraerse a la realidad que estamos viviendo, pero, tanto este año como el pasado, las ciberamenazas aparecen en los primeros lugares, no solo por la probabilidad de que ocurran (cada año se producen en mayor número), sino por la gravedad y el impacto de las consecuencias.

En el año 2019 los ciberataques a instalaciones de la administración fueron casi 43.000, de los que unos 3.000 fueron clasificados de muy alto riesgo y 37 fueron críticos. El pasado año 2020 las cifras fueron casi el doble.

Por tanto, entre los retos a los que tendremos que hacer frente está la adaptación de la seguridad nacional a la adopción de tecnologías disruptivas que acompañan a todas las estrategias de digitalización a nivel mundial sumándole todas aquellas cuestiones relativas a la ciberseguridad, muchas de ellas, recogidas en la Estrategia de Ciberseguridad de 2019 y en todos los trabajos que en este ámbito se están desarrollando.

A ese joven actuario que se inicia en su profesión yo le diría que preste atención a este tipo de riesgos y de la capacidad que tienen las empresas para hacer frente a este tipo de riesgos. Cada día este tipo de riesgos deberá ser más tenido en cuenta a la hora de valorar una operación o una entidad. ●

MIGUEL ÁNGEL BALLESTEROS MARTÍN

Es el Director del Departamento de Seguridad Nacional en el Gabinete del Presidente del Gobierno.

Desde mayo de 2009 hasta junio de 2018 ha sido Director del Instituto Español de Estudios Estratégicos de España, encuadrado en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

Es General de Brigada de Artillería.

Ha sido profesor asociado en la Facultad de Ciencias Políticas y Sociología de la Universidad Complutense de Madrid entre 2015 y 2018, y 17 años profesor en la Universidad Pontificia de Salamanca (Campus de Madrid).

Es doctor en Ciencias Políticas y Sociales por la Universidad Pontificia de Salamanca (Campus de Madrid) con Premio Extraordinario 2015. Es diplomado de Estado Mayor. Es diplomado en Investigación Operativa por la Universidad de Valencia. Ha realizado cursos de especialización en estudios estratégicos en la Universidad de Educación a Distancia de España, en la NATO School en Alemania y en el Colegio de la OTAN (NADEFCOL) en Roma.

También ha realizado cursos de especialización sobre el Sistema de Satélites Helios en París y Toulouse. Es diplomado en Sistemas de Direcciones de Tiro y Detección y Localización de Objetivos.

Además de los destinos como oficial de artillería de campaña y antiaérea, ha estado destinado en el Centro de Investigación Militar Operativa del Ministerio de Defensa, en la División de Inteligencia del Estado Mayor Conjunto de la Defensa. Fue el primer jefe del Centro de Satélites Helios en España. Así mismo fue jefe del Departamento de Estrategia y Relaciones Internacionales de la Escuela Superior de las Fuerzas Armadas en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

Es autor de dos libros: "En busca de una Estrategia de Seguridad Nacional" (Publicaciones Defensa, Madrid 2016) y "Yihadismo" (Editorial la Huerta Grande, Madrid 2016).

Además, es coautor de 33 libros colectivos o monografías, y ha publicado numerosos artículos en revistas especializadas y en diarios como *El País*, *ABC* y *La Razón*.