

PRUEBA DE ACCESO (JUNIO DE 2015)

Cuando el ciberespacio es vulnerable

Las tecnologías de la información y la comunicación se han convertido en una parte central de la vida cotidiana para la mayor parte de la población mundial que afecta incluso a las áreas más atrasadas y remotas del planeta. Son un factor clave para potenciar el desarrollo, la innovación y el crecimiento económico. Sin embargo, estamos solo al principio de una transformación fundamental. En los próximos años, nuevas tecnologías, como el Internet de las cosas, la impresión en 3-D y los vehículos autónomos revolucionarán las prácticas comerciales establecidas, los paradigmas regulatorios e incluso las convenciones sociales.

Estas nuevas tecnologías tienen el potencial de generar enormes beneficios pero también conllevan la asunción de riesgos. El lado negativo de este aumento exponencial de las actividades relacionadas con el ciberespacio es la facilidad de uso y acceso a datos con propósitos criminales.

Existe un consenso acerca de que los ciberataques están aumentando en número, sofisticación, alcance e impacto. A medida que el mundo se vuelve cada vez más interdependiente e hiperconectado se recrudece la preocupación por la vulnerabilidad del ciberespacio. Es una infraestructura de infraestructuras de la que depende el resto de los ámbitos, ya sea la información, el comercio, la energía, el sistema financiero y muchos otros.

Los ciberataques tienen lugar en un medio, el ciberespacio, donde las acciones ofensivas cuentan con ventaja sobre las acciones defensivas. De hecho, la mayor parte de la infraestructura del ciberespacio fue diseñada para asegurar su interoperabilidad y apertura sin centrarse en la seguridad que suele limitar la usabilidad.

Los ataques también tienden a ser asimétricos, debido a las menores barreras de entrada en el ciberespacio y la debilidad de los Gobiernos a la hora de hacer cumplir el Estado de derecho. Esto permite a atacantes con recursos limitados llevar a cabo acciones perturbadoras con mayor impacto que en el mundo físico. Así, los ciberriesgos son transnacionales por naturaleza, ya que tienden a expandirse a nivel global en *efecto cascada* por el alto grado de interconexión e interdependencia entre los actores en el ecosistema digital.

En un medio sin fronteras es imposible abordar con éxito los riesgos desde una sola jurisdicción. La cibercriminalidad ya es un negocio equiparable al tráfico de drogas y altamente internacionalizado. A pesar de ello, no contamos con un régimen de gobernanza global tan desarrollado como en otros ámbitos. Con la intención de paliar este vacío han proliferado distintas iniciativas internacionales para mitigar las ciberamenazas y facilitar la gestión internacional del ciberespacio aunque con un éxito limitado.

En este contexto, las empresas y la sociedad civil tienen un papel que desempeñar a la hora de asegurar una gobernanza abierta, inclusiva y lo suficientemente flexible para adaptarse a la naturaleza cambiante de los ciberriesgos. Es aconsejable hacer hincapié en la preservación de la esfera técnica mientras se adopta un enfoque pragmático en el que se apueste por iniciativas innovadoras pero factibles. Propuestas tales como la creación de un Cíber Consejo de

Estabilidad G-20 (Estados) + 20 (actores no estatales relevantes) o un sistema de alerta temprana y coordinación basado en el modelo de la Organización Mundial de la Salud para las pandemias pueden ser elementos que contribuyan a una mejor gobernanza, como indica el reciente informe de cibergobernanza ESADEgeo y Zúrich.

Responder a las amenazas del siglo XXI con herramientas del siglo XX no parece una buena idea. En 2020 dos terceras partes de la población mundial estarán conectadas y 25 mil millones de objetos *online*. El mundo necesita un diálogo fluido y franco entre Estados, sector privado y sociedad civil para garantizar la seguridad del ciberespacio. Si existen códigos mínimos aceptados a nivel global para regular nuestra vida colectiva no hay razón para que no podamos hacerlo en este nuevo espacio que la tecnología ha puesto a nuestra disposición. La infraestructura del ciberespacio se ha convertido en el equipamiento más importante de nuestro tiempo. Todos tenemos un interés común en preservar su apertura y carácter global. Por eso debiera ser factible superar los intereses nacionales que, a corto plazo, amenazan un progreso colectivo al que no podemos renunciar.

Javier Solana (*El País*, 08-05-2015)

CUESTIONES

1. Elabore un comentario crítico a partir de la tesis defendida por el autor del texto propuesto (un máximo de 40 líneas) (5 puntos).
2. Extraiga del texto dos oraciones de relativo y dos oraciones subordinadas sustantivas. Cópielas y subráyelas en el texto (2.5 puntos).
3. Explique mediante un enunciado o mediante sinónimos el significado de los cinco vocablos subrayados en el texto (2.5 puntos).