

Ciberseguridad

EN 1988, EL USO PÚBLICO DE INTERNET estaba en su infancia y el Reglamento de las Telecomunicaciones Internacionales (RTI) de ese año no contenía disposiciones explícitas sobre ciberseguridad, pero incluía en su Artículo 9 una referencia a la necesidad de evitar “perjuicio técnico” en respuesta a una de las primeras versiones de software malicioso (“malware”), el gusano Morris, que circulaba en esa época. En las décadas transcurridas desde entonces, la importancia de proteger la ciberseguridad ha crecido enormemente y es un tema que será considerado cuando se revise el RTI. Existen propuestas en el sentido de añadir o modificar artículos en el tratado para incluir los elementos relativos a la seguridad, incluidas las medidas contra el correo basura o indeseado (“spam”).

El número y el grado de sofisticación de los ciberataques está aumentando al mismo tiempo que crece nuestra dependencia de Internet y de otras redes para obtener servicios e información críticos. De acuerdo con la compañía de seguridad McAfee, en 2011 se produjo el mayor número de amenazas descubiertas. Se supone que existen aproximadamente unos 70 millones de programas malware circulando en todo el mundo y los teléfonos inteligentes (“smartphones”) se han convertido en el principal medio de su difusión. Los analistas consideran que al menos el 70% de los correos electrónicos son spam.

Mientras tanto, las redes eléctricas inteligentes, la computación en nube, las redes de automatización industrial, los sistemas de transporte inteligentes, la ciberadministración y la banca electrónica, entre otros tipos de infraestructura, se están interconectando. El fallo en uno de esos sistemas afecta a los demás. La mayor facilidad de conexión y la mayor eficacia en las comunicaciones trae consigo una mayor vulnerabilidad frente a los ciberataques¹.

Sin embargo, aún no existe una definición de ciberseguridad aceptada en todo el mundo y ello obstaculiza los esfuerzos de protección que deben emprenderse a nivel nacional e internacional teniendo presente el carácter transfronterizo que tienen hoy en día las redes y sistemas informáticos.

Los incidentes relativos a las tecnologías de la información y la comunicación (TIC) se abordan actualmente con arreglo al derecho penal nacional, que a menudo no está actualizado ni alineado con las tendencias globales. Aún no existe una norma internacional común sobre delitos de esta naturaleza; ¿Deben incluir la piratería del software, por ejemplo, junto con la difusión de la pornografía infantil? ¿El fraude financiero, así como la denegación de los ataques al servicio?. Las respuestas podrían consistir en armonizar las leyes nacionales y establecer un marco jurídico en el que pudiera desarrollarse la cooperación internacional. Sin embargo, algunos consideran que esto no es necesario o que sólo deberían tomarse medidas a nivel regional.

Las leyes no son la única, o la más rápida, respuesta a los ciberataques. Las soluciones técnicas pueden complementarse con normas que logren interoperabilidad y la conformidad con las medidas de seguridad. Esto es especialmente significativo debido a la interdependencia de las redes en el mundo actual. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) ha publicado unas 300 normas referentes a la ciberseguridad. La UIT también ayuda a los países en desarrollo en este tema y apoya la creación de equipos nacionales de intervención en caso de incidente informático. En su Agenda sobre la Ciberseguridad Global², la UIT promueve la cooperación internacional.

Este trabajo forma parte del mandato de la UIT en el sentido de liderar los esfuerzos de coordinación internacional para crear confianza y seguridad en la utilización de las TIC, una tarea que le confiaron los líderes mundiales en los eventos de la Cumbre Mundial sobre la Sociedad de la Información celebrados en 2003 y 2005.

¹ Véase también la Reseña de antecedentes CMTI sobre Protección de la Infraestructura Nacional Crítica.

² Véase www.itu.int/osg/csd/cybersecurity/gca/