La ciberseguridad es algo más que el ciberespacio

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

Seguimos asociando ciberseguridad con la seguridad del ciberespacio, pero cada día que pasa aparecen nuevas realidades que asociadas a la ciberseguridad pero que tienden a desbordarla. En el CIBER elcano de marzo hemos incluido algunas de ellas por su trascendencia para la política de ciberseguridad.

Ana Ayerbe, de Tecnalia, nos habla de la ciberseguridad industrial. Las industrias tienen sus propios problemas de ciberseguridad, diferentes de los del sector de servicios y del resto de usuarios del ciberespacio. Su inseguridad aumenta a medida que la transformación digital y la conectividad afectan a los sistemas de producción y a los productos que fabrican, por lo que las industrias deben tomar medidas para incrementar la resiliencia de los anteriores. Junto a ellas, las industrias y centros tecnológicos dedicados a la seguridad de los sistemas de control industrial deben aprovechar el auge del mercado de la ciberseguridad industrial para asegurarse una parte del negocio.

En la misma línea, Gianluca D'Antonio y Miguel Olías de Lima, de Deloitte, exponen la creciente multidimensionalidad de riesgos a la que se enfrentan las empresas y reivindican el concepto de Seguridad Digital como más comprehensivo que el tradicional de ciberseguridad. La implantación de este concepto tiene efectos en las organizaciones y en el perfil de los responsables de gestionar esos riesgos.

Los efectos, deseados o no, de la transformación digital aumentarán con el despliegue de las redes 5G que analiza Vicente Moret, dentro de un campo de conflicto como es el de la geopolítica digital. En su análisis, se desvelan algunas variables relacionadas con los intereses que existen tras la implantación de las redes, primero, y de las aplicaciones para utilizarlas después. Variables que afectan a la responsabilidad de los gobiernos para garantizar la seguridad de las redes y de las sociedades para competir en el desarrollo de las nuevas tecnologías.

Lo anterior ha sido noticia a lo largo del mes de febrero de 2019 y tiene dos abiertos dos frentes: uno de seguridad, por la fiabilidad de las redes 5G, y otro tecnológico, por su impacto en las aplicaciones tecnológicas que se van a desarrollar para aprovechar las nuevas redes. Con el trasfondo de su guerra comercial con China, Estados Unidos forzó la detención de la responsable de finanzas de Huawei, Meng Wanzhou, en Canadá en diciembre de 2018. Luego prohibió la compra pública de componentes Huawei por razones de seguridad nacional y, en enero de 2019, el director del FBI, Christopher A. Wray,

"La geopolítica digital condujo a Estados Unidos a presionar a sus aliados para ampliar el boicot a las empresas chinas, pero la respuesta no ha sido unánime porque cada uno de ellos tiene unos intereses de seguridad y económicos diferente".

advirtió que la implantación de redes 5G con componentes de Huawei permitiría manipularlas al gobierno chino.

La geopolítica digital condujo a Estados Unidos a presionar a sus aliados para ampliar el boicot a las empresas chinas, pero la respuesta no ha sido unánime porque cada uno de ellos tiene unos intereses de seguridad y económicos diferente. Japón y Australia siguieron la sugerencia y prohibieron la compra pública de productos Huawei y ZTE, mientras que otros como Nueva Zelanda o la República Checa adoptaron medidas similares y se sopesó la posibilidad de que Alemania o el Reino Unido acabaran haciendo lo mismo. Los mayores contratiempos llegaron cuando el responsable del Centro Nacional de Ciberseguridad del Reino Unido declaró que el riesgo de Huawei era manejable, y el responsable de la Agencia Federal de Ciberseguridad de Alemania se mostró partidario de un acuerdo de no espionaje con China.

En el plano bilateral, la controversia se ha traducido en una batalla de comunicación entre Huawei y sus críticos. Huawei alega que no se han encontrado hasta la fecha evidencias que permitan verificar las denuncias estadounidenses, que ha creado laboratorios donde se pueden analizar sus productos y, en consecuencia, ha demandado al gobierno de Estados Unidos por su boicot anticonstitucional.

Con el fondo de la confrontación comercial entre Estados Unidos y China, el problema no está tanto el control de las redes 5G sino en la competencia digital por las aplicaciones que las usan. El negocio está en tener a punto esas aplicaciones para cuando funcionen las redes 5G y se teme que China utilice su ventaja en la instalación de las redes para desplazar a los competidores de sus compañías. Los detractores alegan que las leyes chinas permiten utilizar a esas compañías en funciones de inteligencia y que China obliga a las compañías tecnológica extranjeras a realizar trasferencias tecnológicas que benefician a los competidores chinos. Esta situación, podría cambiar si, como adelanta la agencia Associated Press, China va a cancelar esa exigencia, ya que la legislación que sirvió para despegar su capacidad tecnológica se convierte ahora en un obstáculo para la expansión comercial, lo que ha creado tensiones entre los empresarios chinos y los dirigentes del Partido Comunista de China.

Febrero también nos trajo la mala noticia de los ciberataques rusos sobre *think-tanks* europeos. Se han atribuido al grupo pro ruso APT28 (Fancy Bears) y ha afectado a centros como el German Council on Foreign Relations, las oficinas europeas de los centros estadounidenses German Marshall Fund y Aspen Institute, así como el Institute for Statecraft del Reino Unido. Los ciberataques van dirigidos contra los centros de análisis que han criticado las políticas rusas y, también, a erosionar la credibilidad de las instituciones y procesos democráticos. A los anteriores, hay que añadir los ciberataques norcoreanos sobre *think-tanks* que colaboran con el gobierno de Estados Unidos en relación con los programas de proliferación nuclear de Corea del Norte.

Como se ve, al menos desde CIBER elcano, el reto consiste en contar con la capacidad necesaria para auditar las redes 5G (ciberseguridad) pero también en aprovechar las oportunidades de negocio de esas redes para la industria y la tecnología nacional.