La UE ya tiene una evaluación de los riesgos 5G (ahora falta tomar medidas)

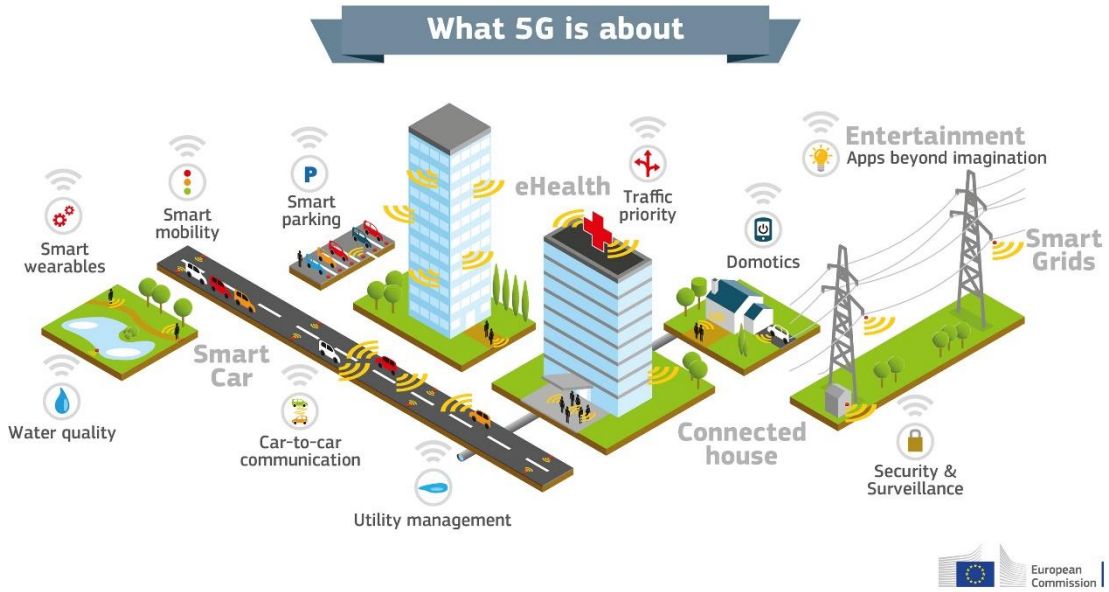
Félix Arteaga | Investigador principal, Real Instituto Elcano.

> "Las nuevas tecnologías 5G aumentan la superficie de exposición de las redes actuales, la sensibilidad y la vulnerabilidad de los componentes ante nuevas amenazas (actores) y riesgos (integridad, disponibilidad y confidencialidad)".

La Comisión acaba de hacer público un informe con su análisis de riesgos de la ciberseguridad de las redes de quinta generación (5G), elaborado sobre las valoraciones de los Estados miembros y con la colaboración de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés)[1]. En 2016 presentó su plan de acción para dotar a la UE de unas infraestructuras digitales de quinta generación (5G) cuyo diseño incidía en elementos claves para el despliegue, pero sin contemplar como punto central la seguridad. Sólo posteriormente, y en medio de la creciente controversia geopolítica sobre el despliegue de redes con componentes de Huawei, se ha reconocido la necesidad de evaluar los riesgos de seguridad de las nuevas infraestructuras. En su comunicación de marzo de 2019, se pedía a los Estados miembros que evaluaran la seguridad de las redes 5G para el 30 de junio de 2019 junto con los requisitos de seguridad y los métodos de análisis de riesgos que van a aplicar. La elaboración se realizó a petición del Consejo Europeo del mismo mes para que el Grupo de cooperación NIS pudiera definir a finales de año tanto las medidas necesarias para mitigar los riesgos, como los requisitos mínimos de seguridad exigibles.

Las evaluaciones nacionales debían identificar los principales activos, amenazas y actores de las redes 5G, así como la sensibilidad y vulnerabilidad de sus distintos componentes, incluidas las derivadas de las cadenas de suministro. Podían contar para ello con las valoraciones de los reguladores y, en su caso, de los operadores y proveedores asociados a las infraestructuras.

[1] ENISA está elaborando un informe sobre algunos aspectos técnicos que complementará el informe actual.



Fuente: Comisión Europea, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/5g_joint_declaration_-_what_5g_is_about_2800px_0.jpg

Las nuevas infraestructuras de red 5G utilizarán tecnologías virtualizadas, cuyos nodos físicos se sustituirán por una nueva arquitectura en la que los protocolos de red se establezcan y ejecuten mediante programas de *software* (virtualización de funciones de red o NFV) en servidores de carácter general (redes definidas por *software* o SDN). Este nuevo paradigma ofrece gran flexibilidad, escalabilidad y capacidad de especialización orientadas a proporcionar con agilidad servicios innovadores y especializados, además de mejoras en eficiencia en costes de operación (OPEX) y de inversión (CAPEX) con respecto a las tecnologías actuales. También facilita la actualización y el parcheo del *software*, pero, en contrapartida, aumenta la exposición de las funciones de red a ciberataques si los desarrolladores del *software* no integran la seguridad desde el diseño inicial. La virtualización permite segmentar los servicios de red (*network slicing*) a la medida de los dispositivos finales o las necesidades de los distintos verticales (p. ej. acceso a internet, industria 4.0, redes corporativas, etc.), pero a costa de aumentar la superficie de exposición al riesgo. La descentralización de la arquitectura de red móvil (*mobile edge computing*) permite reducir la latencia y dotar de inteligencia a una red de acceso 5G muy capilarizada para ofrecer cobertura y capacidad de procesamiento a miles de dispositivos conectados (IoT) a cambio de descentralizar y rebajar las exigencias de los controles de seguridad característicos del núcleo de una red actual.

No son riesgos insalvables, pero, como señala el informe, complican la seguridad porque alargan las cadenas de suministro al incorporar a muchos actores con distintas culturas en ciberseguridad (entre otros, operadores de redes móviles, proveedores de servicios, infraestructuras y contenidos, fabricantes de equipos IT, integradores, proveedores de *software* y servicios *cloud*, usuarios finales…). Las nuevas tecnologías 5G aumentan la superficie de exposición de las redes actuales, la sensibilidad y la vulnerabilidad de los componentes ante nuevas amenazas (actores) y riesgos (integridad, disponibilidad y confidencialidad).

En contra de lo que se podía esperar de un informe elaborado en medio de una creciente competencia geopolítica y del que se esperaban identificaciones concretas sobre la evaluación de los escenarios de riesgos y amenazas, resulta bastante genérico y la identificación de amenazas y actores, casi elemental. El informe reconoce que las valoraciones nacionales han identificado, como se les pedía, que "ciertos países fuera de la UE representan una ciberamenaza para sus intereses nacionales", pero la consolidación de la Comisión adolece de corrección política y no revela cuáles son esos países. El informe identifica como riesgos principales la disrupción local o global de las redes 5G, el espionaje o desvío del tráfico que circula por ellas y la destrucción o alteración de infraestructuras asociadas a ellas, pero no puede evaluar ni la probabilidad ni el impacto de esos riesgos, porque dependen de numerosos factores que se limita a enunciar. Lo mismo ocurre con los actores, a los que se evalúa en función de sus recursos e intenciones, parámetros de difícil objetivación que conducen al lugar común de que los actores estatales o apoyados por los Estados son siempre los más peligrosos.

La evaluación de la sensibilidad (*sensitivity*) de los componentes de las redes se ordena según su impacto –moderado, alto o crítico– en las funciones del núcleo de red (*core network functions*), en la gestión y coordinación de recursos de los servicios de red (*management and network orchestration*), en otros sistemas de gestión (*management systems and supporting services*), en la red de acceso radio (*radio access network*), en los puntos de intercambio de tráfico de internet (*internetwork exchanges*) o en las funciones de la red de transporte y transmisión (*transport and transmission functions*). En función de la sensibilidad de las categorías anteriores, el informe describe las vulnerabilidades previsibles de las redes 5G. Algunas son comunes a las redes de generaciones anteriores, como la falta de personal cualificado o la debilidad de los controles internos de seguridad, la monodependencia de suministradores y el mantenimiento o el incumplimiento de estándares, aunque añaden a esos viejos problemas un nivel superior de complejidad.

> "los nuevos riesgos y las medidas que adoptar van a crear un modelo de ciberseguridad nuevo en las redes 5G del que se deberán revisar las políticas públicas de regulación, supervisión y atribución de responsabilidades en las cadenas de suministro privadas".

Finalmente, el informe combina los cuatro elementos anteriores –riesgos, actores, sensibilidad y vulnerabilidad– e identifica los escenarios de riesgo a los que se enfrentan las redes 5G derivados de las cadenas de suministro, los tipos de ataques que afrontar, las medidas de ciberseguridad que adoptar y su interacción con otros sistemas e infraestructuras.

Se espera que el Grupo de cooperación NIS, con el apoyo de ENISA, Europol, BEREC (Body of European Regulators for Electronic Communications) y el Centro de Situación e Inteligencia de la UE aprovechen las mejores prácticas nacionales para elaborar un inventario de riesgos y medidas de respuesta. Entre los primeros deben figurar riesgos que afecten a la cadena de suministro, al control de acceso, al *software* o a la exposición a problemas regulatorios en terceros países. Entre las medidas se apuntan pruebas de

control o certificación de *hardware* y *software* y la identificación de suministradores, productos o servicios inseguros.

En conjunto, los nuevos riesgos y las medidas que adoptar van a crear un **modelo de ciberseguridad** nuevo en las redes 5G del que se deberán revisar las políticas públicas de regulación, supervisión y atribución de responsabilidades en las cadenas de suministro privadas. Dado el esfuerzo inversor que deben realizar los operadores de telecomunicaciones, es previsible que se acentúe la tensión entre la comercialización de la red y sus servicios, y la adecuación de los niveles de ciberseguridad que ya ha experimentado la implantación de las redes de generaciones anteriores. También incrementará la dificultad de armonizar las medidas de supervisión adoptadas en los Estados miembros de la UE para evitar que la red 5G cuente con eslabones vulnerables, especialmente si las cadenas de suministro desbordan sus fronteras, dentro y fuera de la UE. Las medidas a tomar se esperan antes de 2020, coincidiendo con el año en que se acaba la cuenta atrás para implantar las redes 5G en la UE.