Las medidas de la UE para proteger las redes 5G (EU Toolbox): se dice el pecado, pero no el pecador

Félix Arteaga | Investigador principal, Real Instituto Elcano.

Tema

La UE acaba de aprobar un conjunto de medidas (EU Toolbox) necesarias para hacer frente a las amenazas (Estados y organizaciones criminales) que pueden explotar los riesgos de ciberseguridad de las redes de quinta generación (5G).

Resumen

La seguridad de las redes 5G se convirtió en un problema para la UE cuando los Estados Unidos excluyeron a empresas chinas como Huawei y ZTE del despliegue en su territorio y pidieron a los países europeos hacer lo mismo. Para adoptar una decisión coordinada, los Estados miembros, junto con la Comisión y la Agencia de Ciberseguridad de la UE (ENISA), evaluaron durante 2019 los riesgos, amenazas, sensibilidad y vulnerabilidad de sus redes de quinta generación (5G). En octubre de 2019 publicaron una evaluación coordinada de los riesgos de ciberseguridad asociados al despliegue de las redes 5G. En enero de 2020 y como continuación de la evaluación anterior, la UE ha presentado un conjunto de medidas (*EU Toolbox of Risk Mitigating Measures*) para mitigar los riesgos señalados. Este ARI describe las medidas propuestas y analiza la *anonimización* de las amenazas que dieron lugar a la evaluación de riesgos y a las medidas propuestas.

Análisis

Las redes, tecnologías y aplicaciones 5G son un activo fundamental para la calidad de la vida cotidiana de los ciudadanos y la competitividad de las empresas de la UE en la economía mundial. Las nuevas infraestructuras de red 5G mejorarán la calidad del acceso (velocidad y latencia), la flexibilidad, la escalabilidad y la eficiencia de las tecnologías actuales, así como la actualización y el parcheo del *software*, pero en contrapartida aumentarán significativamente la exposición a los ciberataques si la seguridad no se integra desde el diseño inicial. En el mismo sentido, la mayor descentralización de la arquitectura de red móvil (*mobile edge computing*) reduce la latencia y aumenta la capacidad de cobertura de dispositivos conectados (Internet of Things, IoT), pero genera una superficie de exposición a los riesgos de seguridad mayor que la de las redes actuales. Finalmente, y debido a que las redes 5G se segmentan (*network slicing*) para ofrecer mayores posibilidades de explotación por operadores y grandes clientes, el incremento de la complejidad del *software* y el alargamiento de las cadenas de suministro aumentan la exposición de las redes frente a terceros hasta ahora ajenos a los operadores de telecomunicaciones.

Cuando la UE presentó en 2016 su plan de acción para dotarse de unas infraestructuras digitales de quinta generación, tuvo más en cuenta los elementos de oportunidad que los de riesgo[1]. Pero a la preocupación por los riesgos previsibles se unió pronto la preocupación de los Estados miembros por permitir o no a la compañía Huawei participar en el despliegue de las redes 5G europeas. Mientras Estados Unidos alegaba que la participación de Huawei en las redes 5G permitía brechas de seguridad que podrían explotar las autoridades chinas, Huawei alegó la falta de pruebas empíricas y su disponibilidad para realizar cuantos ejercicios de trasparencia fueran necesarios. El dilema –incluir o excluir a Huawei– en el despliegue de las redes se acentuó a medida que la UE y los Estados miembros quedaron atrapados entre las presiones políticas y diplomáticas de Washington y la influencia de las inversiones tecnológicas y financieras de China y de Huawei, ya emprendidas desde el 4G por operadores europeos, así como el previsible impacto en la innovación y la digitalización.

Para intentar superar el escenario de descoordinación, la Comisión Europea propuso en marzo de 2019 una "Recomendación sobre la ciberseguridad de las redes 5G" para que los Estados miembros evaluaran los riesgos para su ciberseguridad y los remitieran para su valoración conjunta[2]. En octubre de 2019, el Grupo de Cooperación NIS[3] elaboró un "Informe de coordinación de las valoraciones nacionales" en el que identificaba los riesgos, los actores, los activos críticos y las principales vulnerabilidades[4]. Como se analizó en octubre, el informe se limitaba a recopilar los riesgos sin identificar expresamente ningún actor detrás de ellos (amenaza), al igual que ocurrió en el informe posterior de ENISA en el que se desarrollaban, sin atribución expresa, los distintos riesgos detectados, que se resumen en la Figura 1.

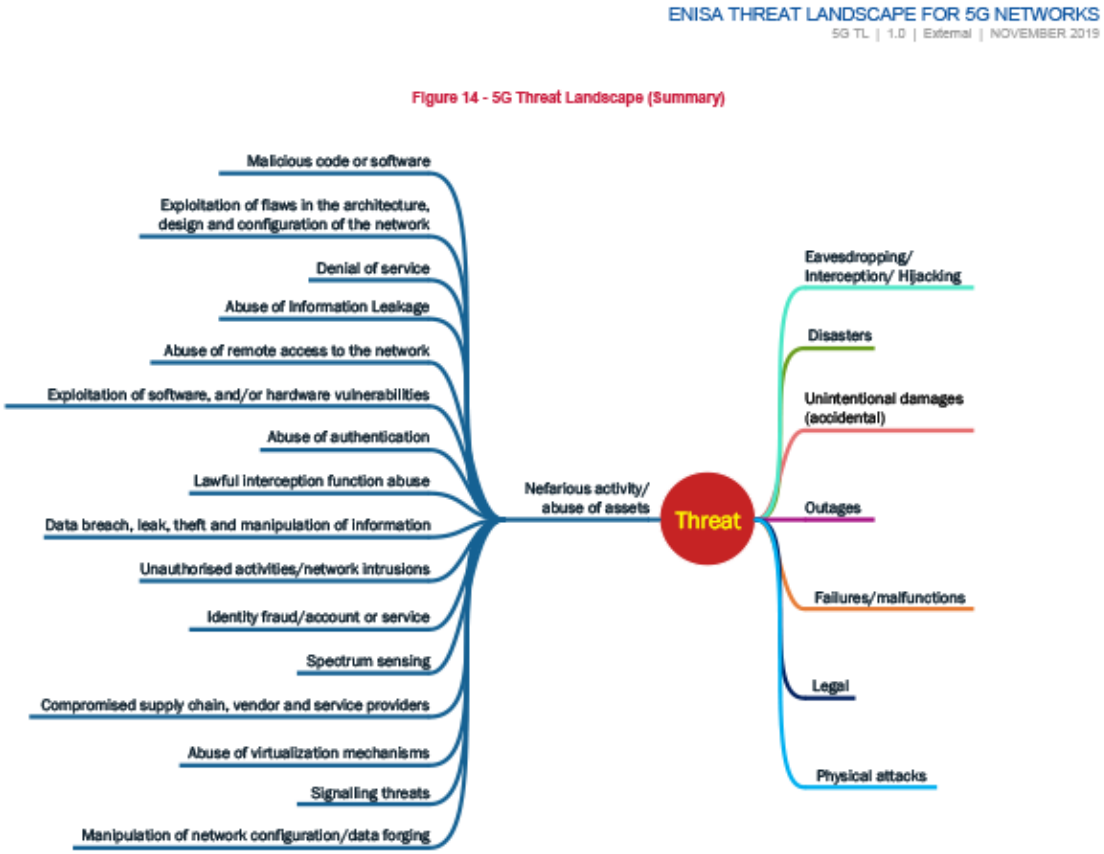
[1] Comisión Europea (2016),"5G for Europe: An Action Plan", COM(2016) 588, de 14 de septiembre, https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/5g-europe.

[2] Comisión Europea (2019), "Cybersecurity of 5G Networks", COM (2019) 534, de 26 de marzo, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA.

[3] El Grupo de Cooperación de la Directiva NIS consta de representantes de los Estados miembros, la Comisión y ENISA bajo la presidencia del Consejo de la UE: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[4] NIS Cooperation Group (2019), "EU coordinated risk assessment of the cybersecurity of 5G networks", 9 de octubre, https://www.europeansources.info/record/eu-coordinated-risk-assessment-of-the-cybersecurity-of-5g-networks.

Figura 1. Mapa de riesgos de las redes 5G



Fuente: ENISA[5].

Como no podía ser de otra forma, las evaluaciones reflejaban un incremento significativo de los riesgos de seguridad en las redes 5G con respecto a la anterior generación 4G; en particular, los que afectaban a su disponibilidad, integridad, privacidad, confidencialidad y accesibilidad, así como los debidos a la multiplicación de suministradores y operadores en las cadenas de suministro o a la inseguridad del suministro debido a la dependencia de un proveedor único. Concretamente, preocupaban los escenarios y categorías de riesgo incluidos en la Figura 2, unos riesgos que se consideraban importantes pero no insuperables si se adoptaban las medidas de seguridad adecuadas.

[5] ENISA (2019), "ENISA threat landscape for 5G Networks", 21 de noviembre, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

Figura 2. Escenarios y categorías de riesgos principales en las redes 5G

Escenarios	Categorías
Medidas de seguridad insuficientes	R1 Desconfiguración de las redes
	R2 Falta de controles de acceso
Cadena de suministro	R3 Baja calidad de los productos
	R4 Dependencia de un proveedor único o falta de diversidad
Modus operandi de los actores detrás de los riesgos (amenazas)	R5 Interferencia estatal a través de la cadena de suministro
	R6 Explotación de las redes o de sus usuarios por organizaciones criminales
Interdependencia entre redes y otros sistemas críticos	R7 Disrupción relevante de las infraestructuras o servicios críticos
	R8 Fallo masivo de las redes debido a la falta de electricidad o de los sistemas de apoyo
Dispositivos de los usuarios finales	R9 Alteración de los dispositivos IoT

Fuente: Elaboración propia sobre datos del "EU Coordinated Risk Assessment Report".

Respecto a las amenazas, es decir, los actores que están detrás de los riesgos y escenarios descritos, las evaluaciones mencionan a los actores accidentales, internos o *hackers* individuales, a los grupos de hacktivistas, terroristas o criminales organizados y a los actores estatales o respaldados por ellos. Este último grupo es el más peligroso para la confidencialidad, disponibilidad e integridad de las redes 5G, pero no se identifican quiénes son las "*certain entitities*" o los "*certain non-EU countries*" que algunas valoraciones señalaron como fuente de riesgo debido a su forma de actuación (*modus operandi*) o a la planificación de sus ciberataques. Se dice el pecado, pero no el pecador, por lo que no se menciona expresamente a China ni a ningún otro país, como Rusia, Corea del Norte o Irán, que responderían a ese patrón de comportamiento según las fuentes abiertas. Las únicas menciones a Huawei solo sirven para ubicarlo entre las grandes compañías suministradoras, junto a Ericsson, Nokia, ZTE, Samsung o Cisco, o para resaltar su colaboración y transparencia con las autoridades británicas de ciberseguridad a propósito de las redes 4G a través del Centro de Evaluación de Ciberseguridad de Huawei en el Reino Unido[6].

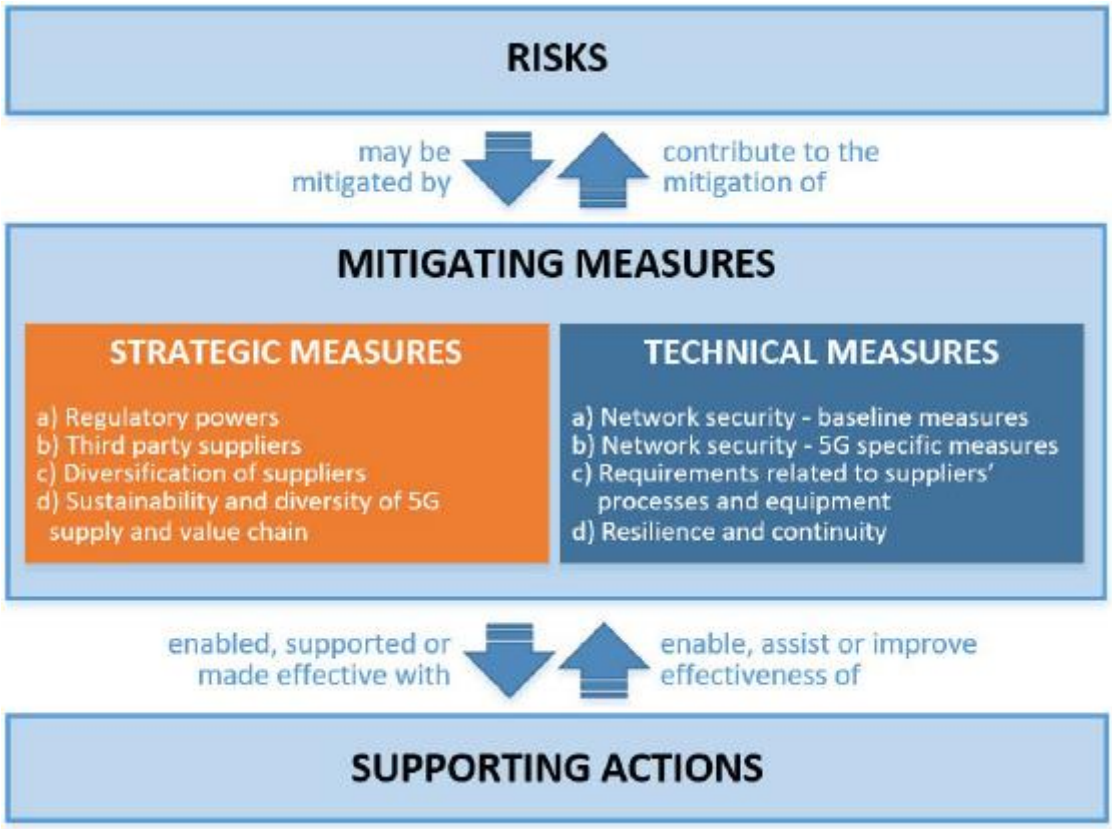
[6] El Huawei Cyber Security Evaluation Centre (HCSEC) emite un informe anual para facilitar la supervisión del National Cyber Security Centre del Reino Unido. El de 2019 (el quinto) se encuentra en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

De los riesgos a las medidas para mitigarlos

Ahora el Grupo de Cooperación NIS propone a la UE y a sus Estados miembros un conjunto de medidas (EU Toolbox) para potenciar la resiliencia de las redes 5G y mitigar los riesgos señalados. En líneas generales, las medidas pretenden integrar la seguridad por diseño en el diseño, despliegue y operación de las redes 5G, aumentar el nivel de exigencia de los estándares de seguridad de los productos y servicios asociados a las redes y reducir los riesgos asociados a suministradores individuales o a su falta de diversidad.

La UE ya cuenta desde hace más de una década con un conjunto de instrumentos normativos que puede mitigar estos nuevos riesgos. El Marco de Telecomunicaciones de la UE ha recomendado medidas para la reducción de riesgos y propiciado la cooperación de los operadores. El Código de Comunicaciones Electrónicas, que reemplazará al anterior a finales de 2020, contiene medidas aplicables a la seguridad de las redes, la gestión de incidentes y la supervisión. También puede apoyarse en la Directiva NIS, que impone obligaciones similares para los operadores de servicios esenciales, y en el Reglamento de Ciberseguridad (*Cibersecurity Act*), que permite desarrollar un sistema de certificación a escala europea para integrar la seguridad por diseño en los productos, servicios y procesos asociados a las redes 5G.
A las medidas regulatorias anteriores se añaden ahora las medidas estratégicas y técnicas para la gestión de riesgo incluidas en la Figura 3. Entre las primeras se encuentran las que refuerzan el papel de las autoridades nacionales y su capacidad de resiliencia, el control y perfilado de los operadores de activos que se identifiquen como críticos –incluyendo restricciones o exclusiones de los que se consideren de alto riesgo– y la diversificación de las cadenas de suministro, tanto ahora como en el futuro.

Figura 3. Medidas estratégicas y técnicas de reducción de riesgos



Fuente: "Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures", p. 11.

Entre las medidas técnicas se incluyen las que integran la seguridad desde el diseño, controlan el acceso y verifican el cumplimiento de las medidas de seguridad física, virtualización, parcheo y actualización del *software* o certificación de los componentes, productos y servicios asociados a las redes 5G. A unas y otras se añaden actuaciones de apoyo que tienen que ver con la adopción de mejores prácticas de seguridad, estandarización, certificación, intercambio de información, gestión de incidentes y requisitos de compra pública. Finalmente, la EU Toolbox recomienda a los Estados miembros que elaboren unos planes de reducción de riesgos combinando los escenarios y categorías de riesgos de la Figura 1 con las medidas estratégicas y técnicas de la Figura 3, aun cuando su ejecución y su coordinación con las medidas de otros Estados miembros dependa de la voluntad de los responsables de los Estados (autoridades nacionales de ciberseguridad) y del sector privado (principalmente, operadores de telecomunicaciones).

A partir de ahora, los Estados miembros, la Comisión y ENISA deben adoptar las medidas necesarias para hacer frente a los riesgos que ellos mismos han identificado. Deberán imponer requisitos específicos, potenciar la certificación y reforzar los requisitos de seguridad para los operadores y para aquellos suministradores que se consideran de alto riesgo, excluyéndolos cuando sea necesario para reducir los riesgos de los elementos críticos de las redes 5G. Las medidas deben velar también por fomentar la diversificación –y europeización– de las cadenas de suministro, evitando la dependencia de suministradores únicos con un alto perfil de riesgo.

La controversia sobre Huawei

La EU Toolbox no contiene ninguna referencia explícita a Huawei, aunque aparece alguna implícita cuando describe como perfil de alto riesgo el de los proveedores que mantienen una relación estrecha con Gobiernos fuera de la UE, cuando dichos países no cuentan con controles democráticos ni legislativos o no existen acuerdos de seguridad de la información o para la protección de datos. El perfil anterior coincide con el de China –la legislación china obliga a sus empresas a cooperar con el Estado cuando se lo pida– porque, aunque podría aplicarse también a Rusia, Irán o Corea del Norte, ni estos países ni sus empresas pretenden participar en el despliegue de las redes 5G en la UE. Precisamente Estados Unidos, cuyo Departamento de Estado ha acogido bien las medidas de la EU Toolbox[7], pide a la UE que excluya o actúe contra los proveedores con ese perfil de alto riesgo, como ha hecho Estados Unidos al excluir a Huawei y ZTE del despliegue de sus redes 5G por su sometimiento al Partido Comunista de China. El Departamento de Estado, debido al enfoque geopolítico que ha tomado el despliegue de las redes 5G, no comparte el criterio de la EU Toolbox de que los riesgos se pueden gestionar y reducir, porque considera que todas las partes de las redes 5G son críticas y, en consecuencia, aboga por una exclusión expresa.

Sin embargo, la decisión británica sobre Huawei en enero de 2020, a pesar de las presiones diplomáticas del presidente Donald Trump y el secretario de Estado Mike Pompeo días antes del Brexit y del inicio de las negociaciones entre Estados Unidos y el Reino Unido para un acuerdo comercial "especial"[8], refleja bastante fielmente la actitud de los Estados miembros frente a la controversia: gestionar los riesgos detectados siguiendo un criterio técnico en lugar de uno político[9]. La estrategia para gestionar riesgos consiste en blindar el núcleo de las redes 5G –añadido a otras medidas de segmentación, redundancia y respaldo–, pero permitir la participación de los suministradores en aquellas funciones de las redes que no son críticas, por ejemplo el acceso[10]. Este enfoque manifiesta tanto la importancia de potenciar la estandarización internacional de protocolos e interfaces entre los distintos elementos de la red[11] como la estrecha correlación entre la calidad de los desarrollos del *software*, la capacidad de corrección de los errores detectados por el suministrador y el grado de vulnerabilidad de

[7] Michael R. Pompeo (2020), "United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers", 30 de enero, https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers.

[8] Adan Satariano (2020), "Britain Defies Trump Plea to Ban Huawei From 5G Network", *The New York Times*, 28/I/2020, https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html.

[9] James Sullivan (2020), "Huawei, Not All the Way", RUSI Commentary, 27 de enero, https://www.rusi.org/commentary/huawei-not-all-way.

[10] Huawei no participa en el núcleo de la red británica, donde se procesan y almacenan datos sensibles, pero puede suministrar estaciones base y antenas, junto con Ericsson y Nokia, fuera de ese núcleo que transmite datos, pero no los almacena. George Parker y Helen Warrell (2020), "Huawei decision jolts 'special' UK-US relationship at highly sensitive time", *Financial Times*, 29/I/2020, https://www.ft.com/content/5bd4e754-41d4-11ea-bdb5-169ba7be433d.

[11] Marcus Willet (2019), "UK, Huawei and 5G: six myths debunked", ISS, 28 de enero, https://www.iiss.org/blogs/analysis/2020/01/csfc-uk-huawei-and-5g-six-myths-debunked, y Emily Taylor (2019), "Who's afraid of Huawei? Understanding the 5G Security Concerns", Chatham House Expert Comment, 9 de septiembre, https://www.chathamhouse.org/expert/comment/who-s-afraid-huawei-understanding-5g-security-concerns.

las redes 5G frente a ciberataques[12]. También Polonia, otro país muy receptivo a las presiones de Estados Unidos, ha decidido diferenciar la participación en el núcleo duro de la libre competencia en el resto[13].

En línea con los planteamientos anteriores –permitir la presencia de Huawei en las redes 5G pero con restricciones– y desde un punto de vista objetivable, las autoridades nacionales y europeas han de velar por una competencia comercial sostenible entre los distintos suministradores para que ofrezcan al mercado soluciones 5G estandarizadas, de calidad y eficientes junto con la estricta aplicación de esquemas de certificación europeos. En un marco de libre competencia, se espera que cada operador de telecomunicaciones tome sus decisiones en función del apetito de riesgo que desea correr sopesando las garantías de seguridad y los costes que le ofrezca el suministrador 5G de su elección.

Francia ya ha confirmado en 2019 que no excluye a ninguno de sus proveedores actuales, incluido Huawei, y que tomará las decisiones sobre el despliegue caso por caso. Alemania, aunque no ha tomado todavía una decisión oficial, parece poco inclinada a seguir las recomendaciones de Washington. Además, su ministro del Interior, Horst Seehofer, ha advertido de que la exclusión de Huawei demoraría la instalación de las redes 5G unos 10 años, con el consiguiente riesgo económico[14]. Mientras el resto de los países se deciden, los operadores de la UE podrían escapar a la controversia sobre Huawei eligiendo a proveedores europeos como Ericsson o Nokia, tal y como acaba de hacer la operadora francesa Orange. Por su parte, Huawei se ha limitado a dar la bienvenida a las medidas de la EU Toolbox, porque le permiten continuar participando en el despliegue de las redes 5G europeas y porque las decisiones se adoptan en función de los hechos y no de los prejuicios, un argumento ya desarrollado en su documento de respuesta a la evaluación coordinada de riesgos de la UE[15].

Conclusiones

La evaluación coordinada y las medidas de reducción de riesgos (EU Toolbox) orientan pero no determinan las decisiones nacionales sobre la seguridad de sus redes 5G. Permiten una mayor sinergia y coordinación con los países, operadores y proveedores, tanto en el ámbito nacional como en el de la UE, pero los Estados miembros son responsables de las decisiones y de sus resultados. Les toca revisar su marco normativo, su capacidad de análisis de riesgos, adoptar las medidas y planes de mitigación de riesgos que les convengan y supervisar y sostener las medidas adoptadas. También les tocará incluir o excluir a Huawei, sea de una vez por todas o caso por caso,

[12] Herb Lin (2019), "Huawei and Managing 5G Risk", *Lawfare*, 3/IV/2019, https://www.lawfareblog.com/huawei-and-managing-5g-risk.

[13] Reuters (2019), "Poland may vary security demands for different parts of FG", 18/XII/2019, https://www.reuters.com/article/us-poland-5g/poland-may-vary-security-demands-for-different-parts-of-5g-minister-idUSKBN1YM1V7.

[14] Rebeca Staudenmaier (2020), "Germany's Seehofer Warns of 5G delay if Huawei is excluded", *DW News*, 18/I/2020, https://www.dw.com/en/germanys-seehofer-warns-of-5g-delays-if-huawei-is-excluded/a-52050565.

[15] Huawei (2019), "Towards a Trustworthy Foundation to Enhance the Security of EU 5G Networks", https://huawei.eu/e-news/2020/01/index.html.

y afrontar las consecuencias –de seguridad o políticas– de la decisión. Las decisiones y medidas básicas tendrán que adoptarlas los Estados miembros antes del 30 de abril de 2020.

Las medidas nacionales deberían llevarse a cabo en coordinación con las de la Comisión y ENISA si se quieren aprovechar las economías de escala y conseguir sinergias. En todo caso, el Grupo de Coordinación NIS evaluará las decisiones y los resultados el 30 de junio de 2020 y los Estados miembros, junto con la Comisión, harán lo propio con la recomendación de marzo de 2019 antes de recomendar medidas adicionales.

Finalmente, y de acuerdo con el enfoque geopolítico que la Comisión Europea propone para las políticas comunes, la UE deberá plantearse la necesidad de prepararse para competir por las tecnologías de las redes 6G en mejores condiciones que en las que lo ha hecho con las redes 5G[16]. En lugar de preocuparse por coordinar una respuesta frente a Huawei, deberá preocuparse por desarrollar una política industrial y tecnológica que le permita aumentar su autonomía tecnológica en un sector estratégico como es el de los sistemas y redes de información. Hay que preocuparse más por la virtud futura que por los pecados –y los pecadores– actuales.

[16] Las filtraciones sobre la futura política industrial de la Comisión Europea apuntan a que la "revolución industrial" pasa por apoyar tecnologías de "importancia estratégica" como las del 6G. Industry Europe (2020), "Leaked Document reveals EU's Ambitious Industrial Plan", 28/I/2020, https://industryeurope.com/leaked-document-reveals-eu-ambitious-industrial-plan.