ARI 121/2018
13 de noviembre de 2018

Evolución de la agenda de ciberseguridad de la Unión Europea

Javier Alonso Lecuit | Miembro del Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

La agenda de ciberseguridad de la UE ha evolucionado significativamente desde el primer Plan Estratégico de Ciberseguridad en 2013 para incorporar nuevas medidas en defensa de la seguridad, prosperidad y libertades de los ciudadanos frente a las amenazas y vulnerabilidades disruptivas del ciberespacio.

Resumen

La seguridad del ciberespacio excede actualmente el ámbito de la ciberseguridad de redes y sistemas de información y se amplía al terreno de la ciberinteligencia, las amenazas híbridas o la ciberdefensa, con importantes consecuencias para los ciudadanos y los Estados. En respuesta, las autoridades europeas y nacionales amplían las iniciativas estratégicas y legales para hacer frente a este escenario de ciberamenazas que se amplía en extensión y alcance.

Este ARI analiza el actual escenario de ciberamenazas y vulnerabilidades, fruto del avance tecnológico y de la consolidación de ecosistemas en torno a la Red, junto a las acciones que han emprendido los legisladores en defensa de la seguridad nacional y económica y de las libertades civiles de sus ciudadanos en materia de ciberseguridad.

Análisis

La Red se ha convertido en un escenario de competición geopolítica y económica entre Estados donde se entremezclan ciberataques, ciberdelitos y desinformación con un propósito desestabilizador. En un primer estadio, la seguridad en la Red (ciberseguridad) se orientó a proteger la integridad, confidencialidad y disponibilidad de las redes y sistemas de información mediante medidas técnicas de seguridad perimetral. Para ello se utilizaron tecnologías orientadas a la detección rápida y la neutralización de las amenazas, el análisis dinámico de las vulnerabilidades de las redes y una respuesta eficaz ante ciberincidentes maximizando la capacidad de recuperación o resiliencia de los sistemas de información.

Desde 2013, los tipos de amenazas e incidentes se han ampliado significativamente en número y gravedad, sin por ello disminuir el número de ciberataques dirigidos a terminales de usuarios, redes de comunicaciones y sistemas de información, con objetivos muy distintos. Entre otros, la obtención masiva de datos de carácter personal y de secretos comerciales; la manipulación de la opinión pública a través de redes sociales en procesos electorales; el uso de Internet para la preparación y consecución

de ataques terroristas; ciberataques con motivaciones económicas a las corporaciones orquestados con el apoyo de los Estados, o la desestabilización política de los Estados democráticos mediante amenazas híbridas apalancadas en las capacidades de desinformación llevadas a cabo a través del ciberespacio. Esta dinámica se ve acentuada por varios factores que dificultan la gestión de estos nuevos riesgos, tales como la vertiginosa evolución tecnológica, la digitalización de todos los ámbitos de la sociedad y la economía o la inmaterialidad y ausencia de fronteras del ciberespacio.

Desde la perspectiva de las vulnerabilidades, la concienciación y formación de los usuarios sigue siendo el gran talón de Aquiles de la ciberseguridad. A pesar de los esfuerzos realizados por las empresas, instituciones privadas y organismos gubernamentales para impulsar la cultura de la ciberseguridad, el grado de vulnerabilidad aumenta a medida que se acelera la digitalización de la sociedad. Otra fuente de vulnerabilidades de carácter endémico es la dependencia tecnológica por parte de los Estados y las empresas europeas de un reducido número de fabricantes de tecnología avanzada en el diseño de circuitos integrados, equipamiento, *firmware*, sistemas operativos e incluso aplicaciones ofimáticas de uso generalizado, producidas por un número muy reducido de países y desplegadas en las nuevas redes de comunicaciones, los sistemas de información o los terminales, entre otros. Esta concentración del mercado de alta tecnología potencia la existencia de vulnerabilidades, en ocasiones intencionadas, de tipo *zero-day* y puertas traseras a disposición de los servicios de inteligencia de esos Estados, que, con el tiempo, acaban filtrándose y comercializándose para su uso por organizaciones criminales que operan en Internet.

Desde la perspectiva del cambio tecnológico, son conocidas las vulnerabilidades que plantean los dispositivos conectados (Internet de las Cosas, IoT por sus siglas en inglés) a los sistemas de información con los que se comunican debido a diseños que no tienen en cuenta los requisitos de ciberseguridad desde la fase inicial. También aparecen nuevos retos técnicos, y en ocasiones éticos, relacionados con el uso de la Inteligencia Artificial (IA). Las funciones de ciberseguridad a distancia (remotización) plantean asimismo a las compañías clientes y a los responsables del tratamiento de los datos nuevos retos en materia de confidencialidad y protección de datos. El uso por los ciberdelincuentes de algoritmos de IA para la identificación de objetivos y para la preparación y la ejecución de ciberataques probablemente desencadene un salto cualitativo tanto en la virulencia de estos como en los mecanismos para su rápida detección, neutralización y respuesta (*hack-back*). Por otro lado, la posibilidad de contar con ordenadores cuánticos en un futuro relativamente cercano, aunque todavía indeterminado, supondrá una discontinuidad en materia de ciberseguridad, ya que los actuales esquemas de cifrado robusto perderán su validez al poder ser descifrados con rapidez. De ahí que algunos Estados estén ya invirtiendo recursos en la investigación de algoritmos de cifrado poscuántico, es decir, resistentes a las capacidades de descifrado[1].

[1] La Comisión dispone del programa de investigación Flagship, de Quantum Technologies, dentro del programa Horizonte 2020, que lo dota con 132 millones de euros hasta 2020.

(cont.)

En este contexto, para hacer frente al imparable crecimiento de ciberincidentes, la Comisión Europea estableció en 2013 el Plan Estratégico de Ciberseguridad de la UE, por el que designaba nuevas autoridades y normativas para la criminalización y persecución de los delitos cometidos en la Red[2]. Se incrementó la supervisión regulatoria a los proveedores de Internet, se elaboró legislación en apoyo de las fuerzas y cuerpos de seguridad y se definieron los instrumentos de respuesta en materia de ciberseguridad, ciberdiplomacia y ciberdefensa con el objetivo de reforzar la protección y las capacidades de respuesta de personas y Estados.

La Comisión elaboró una directiva sobre la seguridad de las redes y sistemas de información (Directiva NIS) para establecer unas capacidades comunes de apoyo, coordinación y respuesta entre los Estados miembros ante ciberincidentes que afectaran a las redes y sistemas de información utilizados por los operadores de servicios esenciales para la seguridad y la economía nacionales[3]. Posteriormente, en septiembre de 2017, ha revisado la Estrategia Europea de Ciberseguridad y ha aprobado un amplio conjunto de medidas que a continuación se enuncian (The Cybersecurity Package)[4]. La Comisión ha propuesto convertir ENISA en una Agencia Europea de Ciberseguridad con mandato permanente que se encargaría de definir un marco europeo de certificación y estandarización de ciberseguridad en productos y servicios con carácter voluntario para simplificar, reducir costes y barreras administrativas (un proceso de certificación por producto válido en la UE), fomentar la "seguridad por diseño" y mejorar la información facilitada a los usuarios de productos y servicios[5]. La agencia funcionaría como secretaría de la red europea de CSIRT, apoyaría a los Estados en la implementación de la Directiva NIS y en la gestión de incidentes y colaboraría en el desarrollo de capacidades y en la concienciación para la prevención de incidentes.

Para reforzar la capacidad de respuesta de la UE y de sus Estados miembros, la Comisión ha propuesto un plan rector (Blue Print) y la creación de un centro europeo de investigación y competencias y de un fondo de respuesta para emergencias de ciberseguridad. También ha liderado una propuesta de cooperación diplomática internacional en materia de ciberseguridad (CyberDiplomacyToolbox) que propone endurecer la respuesta diplomática conjunta de la UE y ampliar el ámbito de estas cibercapacidades a terceros países. En materia de ciberdefensa, la Comisión desea financiar la investigación e innovación en el marco de la Política Común de Seguridad y Defensa (Fondo Europeo de Defensa) y la colaboración con la OTAN.

[2] "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro", JOIN (2013) 1, de 7 de febrero.

[3] Directiva para garantizar la seguridad de las redes y sistemas de información (Directiva NIS), COM (2016) 1148, de 6 de julio, traspuesta mediante Real Decreto Ley 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información (SRI), que se encuentra en desarrollo reglamentario.

[4] "EU Cybersecurity package", 13 de septiembre de 2017.

[5] "The EU cybersecurity certification framework".

(cont.)

Medidas para luchar contra la desinformación en línea

En el curso de los procesos electorales de estos últimos años, al menos 18 países han demostrado la manipulación de su electorado a través de Internet[6]. Desde septiembre de 2015 se han probado 3.900 casos de desinformación favorables a los intereses del Kremlin, es decir, informaciones traducidas a varios idiomas y repetidas diariamente que contradicen hechos constatables por la propia opinión pública[7]. A pesar de que la desinformación es un mecanismo de influencia utilizado desde tiempo atrás, este fenómeno alcanza una nueva magnitud en Internet debido a la capacidad de propagación viral mediante las plataformas *online* y, en particular, las redes sociales para originar y distribuir información falsa con el objetivo de influir en determinados colectivos (la difusión de noticias falsas es un caso particular de desinformación).

En la actualidad, la desinformación a través de noticias falsas en Internet no es un acto penado por la legislación, aunque varios Estados miembros estudian la posibilidad de establecer medidas legislativas. En este sentido, la Comisión ha adoptado sucesivas medidas con creciente determinación desde que presentó en abril de 2018 una comunicación en la que propuso un plan de acción orientado a la protección de procesos democráticos basado en potenciar cuatro principios: la transparencia de las fuentes de información y su financiación, la diversidad de información disponible en Internet y *offline*, la existencia de mecanismos que faciliten verificar la credibilidad de la información y el compromiso duradero de todas las partes que intervienen en el proceso de (des)información[8]. La Comisión solicitó a las plataformas en línea que tuvieran un comportamiento proactivo, proporcionado y responsable para proteger a los usuarios frente a la propagación de noticias falsas, sin incurrir en limitaciones a la libertad de expresión, un comportamiento que evaluará a finales de 2018 con el propósito de adoptar medidas más agresivas si lo considera necesario.

En España, la actual Estrategia de Seguridad Nacional, aprobada en diciembre de 2017, hace referencia a las campañas de desinformación como parte de una estrategia planificada de guerra híbrida que combina desde las fuerzas convencionales hasta la presión económica o los ciberataques. También hace alusión al fenómeno de la posverdad, que intenta movilizar las emociones desdeñando el rigor de los hechos y en la que "la manipulación de la información por parte de agentes externos ejerce de factor de influencia en la era de la posverdad, con efectos negativos en la cohesión social y la estabilidad política".

Medidas para garantizar la ciberseguridad de las elecciones europeas

La Comisión Europea ha mostrado una gran preocupación por proteger los procesos electorales, en particular las elecciones europeas en mayo de 2019, del riesgo que constituyen los ciberataques dirigidos a los sistemas de información utilizados por partidos políticos, candidatos o las propias administraciones públicas en las campañas

[6] "Freedom on the net report 2017", Freedom House.

[7] UE East StratCom Task Force, European External Service.

[8] Comunicación sobre "Tackling online disinformation: a European Approach", COM (2018) 236, de 26 de abril.

(cont.)

y procesos electorales, ataques que pueden afectar a la integridad y la equidad del proceso electoral[9]. El 12 de septiembre de 2018 la Comisión propuso un conjunto de medidas para garantizar unas elecciones europeas libres y justas frente a riesgos como el de campañas masivas de desinformación en línea que persiguen desacreditar y deslegitimar elecciones, tal como se ha visto en el punto anterior; el uso ilícito de los datos personales, y los ataques contra la infraestructura electoral y los sistemas de información de campaña, riesgos que constituyen en su conjunto amenazas híbridas habitualmente orquestadas desde Estados externos a la UE con propósitos desestabilizadores.

La Comisión ha elaborado, junto con las administraciones nacionales responsables de la ciberseguridad y ENISA, orientaciones específicas sobre las amenazas a la ciberseguridad, una comunicación con el fin de potenciar las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación, así como orientaciones sobre la aplicación del Reglamento General de Protección de Datos de la UE y una enmienda legislativa que hace más rigurosas las normas sobre la financiación de los partidos políticos europeos[10]. La Comisión insta a las autoridades nacionales, los partidos políticos y los medios de comunicación a que también adopten medidas para proteger sus redes y sistemas de información de amenazas de ciberseguridad.

Por su parte, el Grupo de Cooperación de la Directiva NIS, compuesto por un representante de cada Estado miembro y representantes de la Comisión y de ENISA, emitió en julio de 2018 un informe orientado a facilitar directrices de ciberseguridad y de gestión de incidentes, así como potenciar la cooperación estratégica entre los Estados, en relación con la seguridad de las redes y sistemas de información utilizados en las elecciones[11]. Acompañando este conjunto de recomendaciones, la Comisión ha propuesto un reglamento para poner en común recursos y conocimientos técnicos en tecnologías de ciberseguridad[12]. La Comisión plantea crear una Red de Centros de Competencia en Ciberseguridad con el fin de canalizar y coordinar mejor la financiación disponible para la cooperación, investigación e innovación en materia de ciberseguridad. Un nuevo Centro Europeo de Competencia en Ciberseguridad gestionará la ayuda económica con cargo al presupuesto de la UE destinado a ciberseguridad, lo que fomentará la inversión conjunta de la Unión, los Estados miembros y empresas del sector para fortalecer la industria de ciberseguridad de la UE y asegurar que los sistemas de defensa incorporen las técnicas más avanzadas.

[9] "Estado de la Unión 2018". Seguridad en los procesos electorales.

[10] Comunicación para garantizar unas elecciones europeas libres y justas, COM (2018) 637, de 12 de septiembre de 2018.

[11] "Compendium on Cyber Security of Election Technology", CG Publication 03/2018, NIS Cooperation Group, julio de 2018.

[12] Propuesta para una "Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM (2018) 630, de 12 de septiembre.

(cont.)

La prevención de la difusión de contenidos terroristas en línea

La Comisión Europea incluyó en el paquete de medidas en materia de ciberseguridad presentado en septiembre de 2017 una comunicación con un conjunto de directrices y principios encaminados a potenciar la proactividad de las plataformas en línea a la hora de prevenir, detectar y eliminar contenidos ilícitos en la Red que inciten al odio, la violencia o el terrorismo[13]. Esta comunicación era el primer paso de un proceso por el que iba a monitorizar la proactividad y el progreso experimentado en las plataformas de Internet durante los próximos meses para evaluar la posible necesidad de adoptar medidas adicionales que garanticen una rápida detección y eliminación de contenidos ilícitos en línea, incluyendo posibles medidas legislativas.

A tenor de los resultados obtenidos, la Comisión emitió en marzo de 2018 una recomendación para la adopción de un conjunto de medidas operativas más estrictas[14]; entre otras, la adopción por los proveedores de procedimientos más claros de «notificación y acción» a fin de evitar que se retiren de forma accidental contenidos que no sean ilícitos; instrumentos proactivos para detectar y retirar los contenidos ilícitos, en particular contenidos terroristas o aquellos que no necesiten contextualización para considerarse ilícitos (por ejemplo, el material relacionado con abusos sexuales a menores o las mercancías falsificadas); salvaguardias más sólidas para garantizar los derechos fundamentales, y, en particular, la supervisión y verificación por humanos de mecanismos automatizados de detección y retirada de contenidos. La Comisión hizo un llamamiento a la cooperación más estrecha entre las distintas autoridades y a compartir las mejores prácticas en beneficio de las plataformas de menor tamaño, que habitualmente cuentan con unos recursos y unos conocimientos técnicos más limitados.

Asimismo, la Comisión propuso en septiembre de 2018 la adopción de un reglamento para la prevención de la difusión de contenidos terroristas en línea que establece como medida central la obligación de todas las empresas *online* a retirarlos, como norma general, en el plazo de una hora desde su notificación[15]. Además, las empresas de Internet deberán introducir medidas proactivas, principalmente basadas en la detección automatizada, para retirar los contenidos terroristas o inhabilitar el acceso a ellos de manera eficaz y rápida y evitar que vuelvan a aparecer una vez hayan sido retirados. A fin de ayudar a las plataformas más pequeñas, las empresas han de compartir y optimizar los instrumentos informáticos adecuados y poner en marcha acuerdos de colaboración que favorezcan una mayor cooperación con las autoridades pertinentes, en particular con Europol. El reglamento insta a los Estados miembros a introducir nuevos procedimientos para tramitar las notificaciones con la mayor rapidez posible y

[13] Comunicación sobre "Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms", COM (2017) 555, de 28 de septiembre.

[14] Recomendación sobre "Measures to effectively tackle illegal content online", COM (2018) 1177, de 1 de marzo.

[15] Propuesta de Reglamento para la prevención de la difusión de contenidos terroristas en línea, COM (2018) 640 de 12 de septiembre.

(cont.)

asegurarse de disponer de las capacidades y los recursos necesarios para detectar, identificar y notificar los contenidos terroristas[16].

Medidas para la regulación del acceso a pruebas electrónicas

Las investigaciones policiales y judiciales de la UE se desarrollan en un contexto en el que más del 50% de las investigaciones penales incluyen —al menos— una solicitud transfronteriza para la obtención de pruebas electrónicas que obran en poder de prestadores de servicios establecidos en otro Estado miembro o externo a la UE. Casi dos terceras partes de los delitos cuyas pruebas electrónicas se encuentran en otro país no pueden ser debidamente investigados o enjuiciados debido al tiempo necesario para recabar tales pruebas o debido a la fragmentación del marco jurídico, en el que la cooperación público-privada entre proveedores y autoridades es ineficiente, no existe un marco legal para la cooperación voluntaria trasfronteriza y no hay suficiente certeza legal sobre el uso de pruebas electrónicas en investigaciones transfronterizas. Para contrarrestar ese entorno tan perjudicial para las investigaciones, la CE propuso en abril de 2018 dos normas para facilitar a las autoridades policiales y judiciales la obtención de pruebas electrónicas necesarias para investigar, enjuiciar y condenar a delincuentes y organizaciones terroristas: un reglamento para el acceso transfronterizo a pruebas electrónicas (*e-evidence*) y una directiva que lo complementa con el propósito de armonizar la designación de los representantes legales de las compañías en línea[17].

El reglamento establece una orden de producción europea para la entrega de pruebas electrónicas en investigaciones transfronterizas que permitirá a la autoridad judicial de un Estado miembro solicitarlas directamente al prestador de servicios establecido en otro Estado de la Unión, con independencia de la ubicación de los datos. El prestador habrá de responder en 10 días máximo o en 6 horas en casos excepcionales. Asimismo, prevé una orden de producción de ámbito europeo para la conservación de las pruebas electrónicas en el curso de una investigación que impida el borrado de los datos. El reglamento se dirige a aquellos prestadores de servicios de información cuyo elemento definitorio del servicio que ofrecen sea el almacenamiento de datos. Incluye, entre otros, a proveedores de comunicaciones electrónicas, *hosting* y almacenamiento en la nube, redes de distribución de contenidos, plataformas de redes sociales, mercados *online* orientados a consumidores finales y negocios, comunicaciones vocales y proveedores de infraestructuras de Internet. El reglamento obliga a designar un representante legal en la UE, incluye garantías procesales y vías de recurso para la protección de los derechos fundamentales y ofrece seguridad jurídica tanto para las autoridades como para los prestadores de servicios.

[16] Es importante señalar que la recomendación no modifica la Directiva de Comercio Electrónico de 2000 en lo relativo a la exoneración —con carácter general— de las responsabilidades de las plataformas *online* en relación con los contenidos de la información gestionada (principio *mere conduit*).

[17] Propuesta para la "Regulation on European Production and Preservation Orders for electronic evidence in criminal matters", COM (2018) 225, de 17 de abril, y propuesta para una "Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226, de 17 de abril.

Conclusiones

En un contexto creciente de amenazas y vulnerabilidades en el que la seguridad del ciberespacio excede actualmente el mero ámbito de la ciberseguridad de redes y sistemas de información, las autoridades europeas y nacionales amplían las iniciativas estratégicas y legales para hacer frente a este escenario cada vez mayor de ciberamenazas, lo que muestra la necesidad de supervisar y regular en determinadas situaciones a los proveedores de Internet. En este sentido, la Directiva NIS instaba a la revisión de las estrategias de ciberseguridad de los Estados para adaptarlas al nuevo escenario.

Las estrategias de ciberseguridad ofrecen un enfoque de seguridad nacional del ciberespacio centrado en la obligación del Estado de asegurar el funcionamiento de los servicios públicos, las infraestructuras críticas, las redes y sistemas y la privacidad y los derechos digitales del ciudadano. Sin embargo, son las empresas privadas las encargadas de proteger las redes y sistemas de información utilizados para ofrecer servicios esenciales. Por ello, resulta vital fortalecer los mecanismos de colaboración entre las instituciones y el sector privado.

El gobierno español aprobó en agosto de 2018 un Acuerdo del Consejo de Seguridad Nacional por el que se aprueba el procedimiento para la revisión de la Estrategia de Ciberseguridad Nacional de 2013[18]. En él se considera la participación de un comité de expertos independientes en la fase de revisión del borrador elaborado por un Comité Técnico de la Administración. Este procedimiento de doble instancia agiliza la tramitación, pero no garantiza que el texto final responda a una visión compartida por el sector público y el privado respecto a los riesgos de ciberseguridad conocidos y emergentes que se han mencionado.

[18] Procedimiento para la elaboración de una nueva Estrategia de Ciberseguridad Nacional, PCI/870/2018, de 3 de agosto, que sustituya a la Estrategia Nacional de Ciberseguridad vigente, de 2013.