Documento
Opinión

75/2023 18 de septiembre de 2023

Marian Soto Soriguera *

Nuevas tecnologías en el contexto global de seguridad: la oportunidad frente al desafío

Nuevas tecnologías en el contexto global de seguridad: la oportunidad frente al desafío

Resumen:

Nos encontramos inmersos en un proceso de cambio global determinado por la irrupción de nuevas tecnologías que están provocando una rápida evolución en la forma de relacionarse en todos los ámbitos. Estos cambios suponen un avance de lo físico a lo digital, de lo paulatino a lo inmediato, de lo palpable a lo intangible.

Todo ello influye de forma determinante en la conformación del nuevo sistema de seguridad global, donde los avances tecnológicos de nueva generación ofrecen oportunidades, pero también suponen desafíos derivados de las disputas por su control, de su uso con fines ilícitos o relacionados con la ampliación del espacio de vulnerabilidad a medida que aumenta la conectividad.

En el presente artículo se abordan la transformación digital y sus efectos más importantes, su influencia en la morfología de los riesgos y amenazas para la seguridad y el enfoque que se da a este fenómeno desde las políticas de seguridad de países como España.

Palabras clave:

Tecnología, seguridad, estrategia, transformación digital, inteligencia artificial, oportunidad, desafío.

New technologies in the global security context: the opportunity facing the challenge

Abstract:

We are immersed in a process of global change determined by the irruption of new technologies, which are causing a rapid evolution in the way of relating in all areas. Changes that represent an advance from the physical to the digital, from the gradual to the immediate, from the tangible to the intangible.

All of this has a decisive influence on the conformation of the new global security system, where next-generation technological advances offer opportunities, but also challenges derived from disputes over their control, their use for illicit purposes or related to the expansion of the space of vulnerability as connectivity increases.

This article addresses the digital transformation and its most important effects, its influence on the morphology of security risks and threats, as well as the approach taken from the security policies of countries such as Spain.

Keywords:

Technology, security, strategy, digital transformation, artificial intelligence, opportunity, challenge.

Cómo citar este documento:

SOTO SORIGUERA, Marian. *Nuevas tecnologías en el contexto global de seguridad: la oportunidad frente al desafío*. Documento de Opinión IEEE 75/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO75_2023_MARSOT_Tecnologias.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción. La transformación digital como vector de cambio

En 2016, Klaus Schwab, fundador y presidente ejecutivo del Fondo Monetario Internacional, señalaba que nos encontrábamos «al borde de una revolución tecnológica que cambiará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos unos con otros»[1].

Tecnologías disruptivas como la inteligencia artificial[2] o el internet de las cosas *(internet of things)*[3] forman parte de nuestro día a día y nos ofrecen formas más ágiles de actuar y avances impensables hace pocos años en el modo de interactuar, desarrollar o crear en todas las esferas de nuestra vida cotidiana.

Esta evolución exponencial en el desarrollo global se encuadra en lo que Schwab identificaba como la «Cuarta Revolución Industrial», caracterizada por «una fusión de tecnologías que está desdibujando las líneas entre las esferas física, digital y biológica»[4].

Por tanto, sorteando diversas etapas intermedias, pasamos del vapor y la energía hidráulica como motor del cambio en la Primera Revolución Industrial del siglo XVIII al impulso decidido del proceso de digitalización en el siglo XXI, con el dato como fundamento de todos los procesos de gestión tecnológica y con un gran potencial de crecimiento en ámbitos como la economía o la industria, basado en la adopción de modelos productivos sustentados en la automatización.

[1] SCHWAB, K. «The Fourth Industrial Revolution: what it means, how to respond». World Economic Forum, 14 de enero de 2016. Disponible en: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ [consulta: 15/7/2023].

[2] No existe aún una definición formal y universalmente aceptada de *inteligencia artificial*. La Comisión Europea se ha referido a ella como «sistemas de *software* diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital: percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de inteligencia artificial pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas» (*AI Watch: Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence.* 2020, pp. 8-9. Disponible en: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118163/jrc118163_ai_watch._defining_artificial_intelligence_1.pdf [consulta: 15/7/2023]).

[3] El *internet de las cosas* se refiere a la red de objetos físicos que pueden conectarse e intercambiar datos con otros dispositivos y sistemas a través de internet.

[4] SCHWAB, K. *Op. cit.*

En esta última etapa discurre el proceso de transformación digital, fruto de la implementación de nuevas tecnologías, que tiene un protagonismo creciente en la sociedad.

En dicho contexto, la Unión Europea (UE) busca ser líder mundial en la carrera tecnológica y considera la transformación digital como una de sus prioridades de actuación. Con este fin, en los últimos años, se están impulsando acciones orientadas a garantizar la innovación en el marco de la denominada Década Digital de Europa[5], que genera nuevas oportunidades y, por encima de todo, sitúa a las personas y sus derechos en el centro de la transformación digital.

Ciñéndose a las premisas expuestas, el programa político de la UE tiene como finalidad orientar la transformación digital de Europa hasta 2030 en cuatro direcciones: una población con capacidades y unos profesionales digitales altamente cualificados, unas infraestructuras digitales seguras y sostenibles, la transformación digital de las empresas y, por último, la digitalización de los servicios públicos.

Figura 1. Metas y objetivos de la Década Digital de la Unión Europea (hasta 2030)
Fuente: COMISIÓN EUROPEA. Disponible en: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030 [consulta: 15/7/2023].

[5] DECISIÓN (UE) 2022/2481 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030. Diario Oficial de la Unión Europea. L 323, 19 de diciembre de 2022 [consulta: 15 /7/2023].

En línea con lo anterior y para dar respuesta a las nuevas necesidades, el Gobierno de España aprobó la agenda España Digital 2020, posteriormente actualizada con un horizonte temporal más amplio: España Digital 2026[6]. Esta agenda aborda la transformación digital como un pilar estratégico para la recuperación de la crisis derivada de la COVID-19, además de ser una de las palancas principales para la innovación tecnológica, el desarrollo empresarial, la modernización económica y el progreso social.

Desde su puesta en marcha, se han adoptado numerosas medidas en muy diversos ámbitos. Entre otras, por su trascendencia para la seguridad, cabe destacar las recogidas en el Plan Nacional de Ciberseguridad[7] o el Plan de Choque de Ciberseguridad[8], que pretenden fortalecer las capacidades de ciberseguridad de la ciudadanía, las pymes y los profesionales e implantar nuevas capacidades de prevención, preparación y respuesta.

A continuación se desglosan las características de este proceso de digitalización y los avances de las tecnologías emergentes.

Sociedades hiperconectadas

Estamos en un mundo hiperconectado donde internet se está convirtiendo en algo tan indispensable como la electricidad. El avance exponencial en los últimos años de la conexión digital en las actividades públicas, privadas y profesionales ha consolidado la conectividad como rasgo definitorio de la sociedad actual.

Tras su impulso durante los años de mayor incidencia de la pandemia, los hábitos de consumo de internet en el mundo se siguen afianzando y el servicio alcanza a un número

[6] GOBIERNO DE ESPAÑA. España Digital 2026. Disponible en: https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf [consulta: 17/7/2023].

[7] GOBIERNO DE ESPAÑA. Plan Nacional de Ciberseguridad, Acuerdo de Consejo de Ministros de 29 de marzo de 2022. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2022/refc20220329_corregidav02.aspx#ciberseguridad [consulta: 12/7/2023].
Este plan cumple el mandato emitido por el Consejo de Seguridad Nacional, en su reunión del 18 de noviembre de 2021 y desarrolla lo establecido por la Estrategia Nacional de Ciberseguridad 2019, documento estratégico en el que se desarrollan las previsiones en el ámbito de la ciberseguridad. En concreto, recoge un centenar de iniciativas para su ejecución en los próximos tres años, vinculadas en su mayor parte al Plan de Recuperación, Transformación y Resiliencia, de 16 de junio de 2021.

[8] GOBIERNO DE ESPAÑA. Plan de Choque de Ciberseguridad. 25 de mayo de 2021. Disponible en: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210525_np_ciberseguridad.aspx [consulta: 16/7/2023].

cada vez mayor de personas. Así, el número de usuarios a nivel global alcanza ya los 5160 millones de personas, el 64,4 por ciento de la población mundial. En 2023, la cifra global de internautas aumentó en 98 millones de personas: un incremento del 1,9 por ciento respecto a las estadísticas de 2022[9].

No obstante, el aumento de la conectividad y del tráfico de datos tiene un importante contrapunto en la situación de los países menos adelantados (LDC, por sus siglas en inglés)[10], donde tan solo el 36 por ciento de la población accede a internet[11], cifra que contrasta con el 65 por ciento que se registra a nivel global. Los 720 millones de personas que siguen sin conexión en los países señalados en el siguiente mapa representan el 27 por ciento de la población mundial sin acceso al servicio, a pesar de que solo conforman el 14 por ciento de la población global.

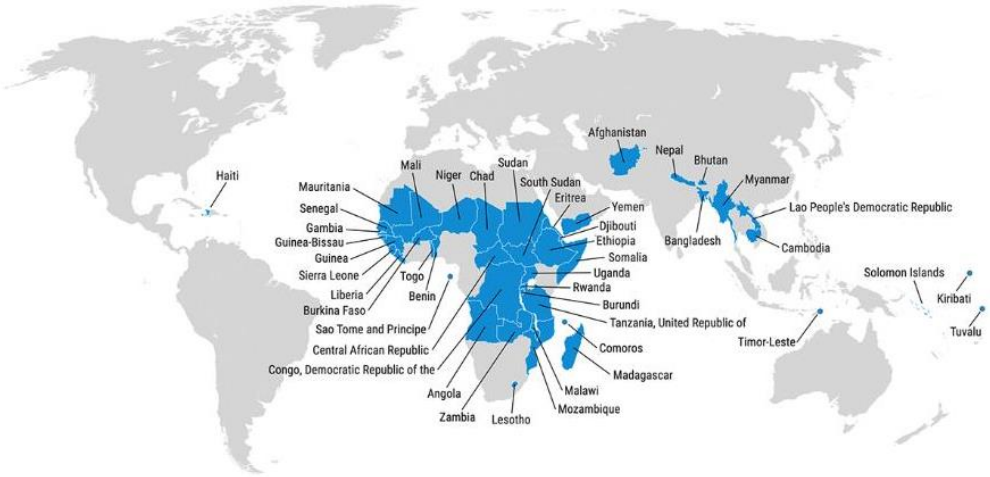

Figura 2. Lista ONU de países LDC
Fuente: CONFERENCIA DE LAS NACIONES UNIDAS SOBRE COMERCIO Y DESARROLLO (UNCTAD). Octubre de 2022. Disponible en: https://unctad.org/topic/least-developed-countries/list [consulta: 15/7/2023].

[9] Esta es una de las principales conclusiones del *Digital Report 2023,* la última edición del estudio anual realizado por We Are Social y Meltwater (Disponible en: https://datareportal.com/reports/digital-2023-global-overview-report [consulta: 18/7/2023].).
[10] Es una categoría de Estados que se consideran muy desfavorecidos en su proceso de desarrollo por razones estructurales, históricas y geográficas. Actualmente, la ONU eleva la cifra a 46 (880 millones de personas, el 12 por ciento de la población mundial).
[11] INTERNATIONAL TELECOMMUNICATION UNION (ITU), TELECOMMUNICATION DEVELOPMENT SECTOR. «Facts and Figures: Focus on Least Developed Countries». Marzo de 2023. Disponible en: https://www.itu.int/itu-d/reports/statistics/facts-figures-for-ldc/ [consulta: 12/7/2023].

La brecha digital, lejos de cerrarse, sigue en aumento. La falta de recursos económicos, de acceso a infraestructuras y de conocimiento o alfabetización digital son las principales causas que propician esta situación.

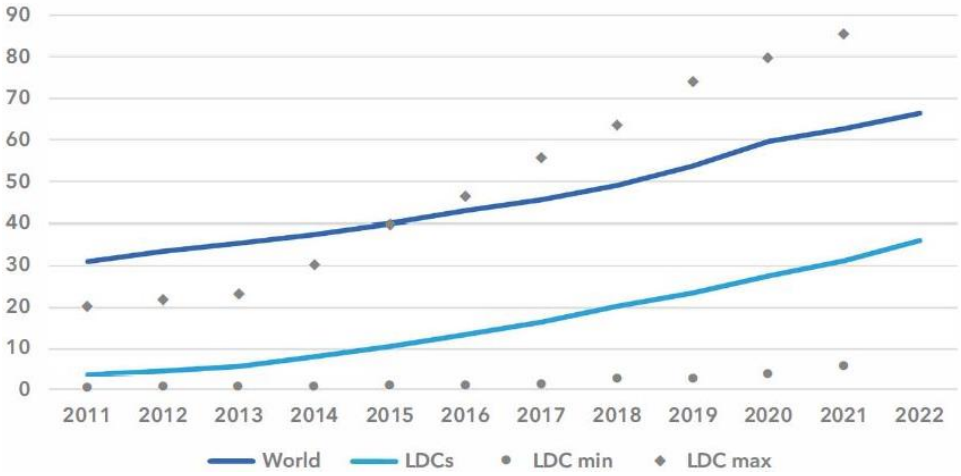

Figura 3. Evolución temporal del porcentaje de los individuos que usan internet a nivel global y en el conjunto de los países LDC
Fuente: INTERNATIONAL TELECOMMUNICATION UNION. «Facts and Figures: Focus on Least Developed Countries». Marzo de 2023 [consulta: 14/7/2023].

Por lo que respecta a su posicionamiento en la carrera tecnológica, España ocupa un lugar destacado dentro de la UE de acuerdo con el Índice de Economía y Sociedad Digital (DESI) 2022[12] de la Comisión Europea.

En cuanto a la conectividad digital, España es uno de los países que mejores resultados obtiene: está a la vanguardia en administración electrónica y servicios públicos digitales en el entorno comunitario y continúa actualizando sus servicios e infraestructura para adaptarlos a los rápidos desarrollos tecnológicos y a las necesidades de las personas y las empresas.

En concreto, España ocupa el puesto 7 entre los Estados miembro. Sus resultados mejoran especialmente en integración de la tecnología digital, puesto 11 (cinco puestos mejor que en 2021); servicios digitales públicos, puesto 5 (frente al puesto 7 de 2021), y en términos de capital humano, puesto 10 (frente al puesto 12 del año precedente).

[12] COMISIÓN EUROPEA. «Report Country Profile: Spain», Índice de Economía y Sociedad Digitales (DESI) 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance [consulta: 14/7/2023].

Además, España es uno de los países líderes de la UE en conectividad, ya que ocupa el puesto 3 por segundo año consecutivo.

	España		UE
	Puesto	Puntuación	Puntuación
DESI 2022	7	60,8	52,3

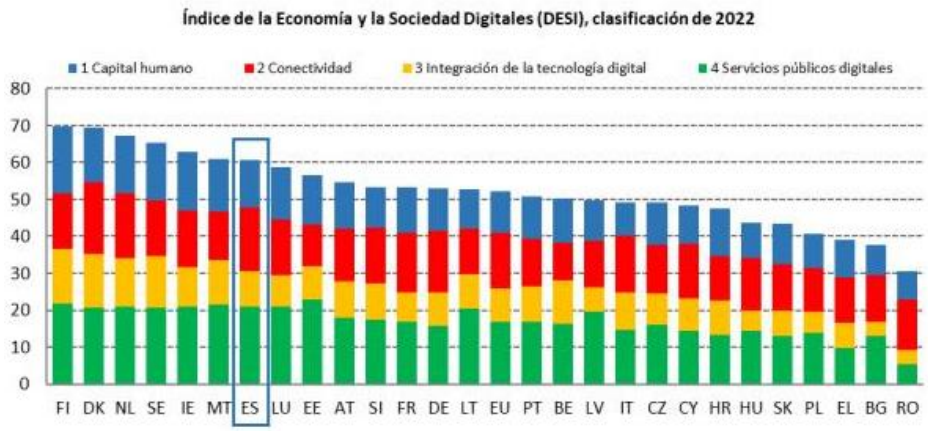

Figura 4. Índice de la Economía y la Sociedad Digitales 2022
Fuente: COMISIÓN EUROPEA. «Report Country Profile: Spain». Disponible en: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance [consulta: 14/7/2023].

Junto a ello, el país sigue avanzando en el despliegue de redes de muy alta capacidad, al tiempo que lleva a cabo reformas e inversiones estratégicas para alcanzar los objetivos de conectividad y reducir la brecha digital entre las zonas urbanas y rurales.

Tecnologías disruptivas

Otra característica del proceso que nos ocupa es el desarrollo de tecnologías disruptivas. Para que una tecnología se considere disruptiva tiene que modificar un hábito o un comportamiento y ser accesible para la mayoría de la población. Son ejemplos de tecnologías disruptivas la inteligencia artificial, en la que se combinan algoritmos programados para que una máquina realice acciones que hasta ahora realizaban los seres humanos, o el mencionado internet de las cosas, una tecnología emergente que adquiere cada vez más protagonismo.

También forman parte de este grupo tecnologías como la cadena de bloques *(blockchain),* que se aplica en flujos de trabajo digitalizados y permite la transferencia

segura de datos codificados a través de la red; la tecnología 5G, que posibilita que los dispositivos estén conectados y compartan información a gran velocidad, o el aprendizaje automático *(machine learning),* disciplina, dentro del campo de la inteligencia artificial, que permite que los ordenadores aprendan por sí mismos y realicen tareas de forma autónoma.

En España, la implementación de las tecnologías citadas es una realidad en constante evolución en los sectores más relacionados con la información y las comunicaciones o con el ámbito científico e industrial, no tanto en otros como las actividades administrativas y auxiliares.

El último informe sobre *Tecnologías digitales en la empresa*[13], que analiza del uso de tecnologías emergentes en las empresas españolas, destaca que la transformación digital de los procesos de negocio toma fuerza en el tejido empresarial nacional.

En concreto, el informe recoge que el 31,8 por ciento de las empresas españolas hace uso de la computación en la nube *(cloud computing),* el 13,9 por ciento de la inteligencia de datos *(big data)* y que un 11,8 por ciento ha implementado en su actividad la inteligencia artificial. Además, un 7,8 por ciento de las empresas emplea robots en los procesos de negocio, mientras que el 30 por ciento realiza ventas telemáticas.

Como contrapunto, las acciones para reducir los riesgos derivados del uso de las nuevas tecnologías no evolucionan al mismo ritmo, y se estima necesario el refuerzo de las medidas de ciberseguridad. En la actualidad, de acuerdo con el informe indicado, el 89,1 por ciento de las empresas de diez o más personas cuenta con alguna medida de este tipo. En el caso de las microempresas, el porcentaje desciende hasta el 55,3 por ciento.

Por último, la prevalencia de criterios distintos a la seguridad en el diseño de productos de *hardware* y *software,* los sistemas y servicios que posibilitan el intercambio de información a gran velocidad, la interconexión de un elevado número de dispositivos, la generación de algoritmos con ingentes cantidades de datos o las actuaciones automatizas por parte de máquinas abren un amplio espacio de vulnerabilidad que precisa de una mayor atención.

[13] GOBIERNO DE ESPAÑA. *Tecnologías digitales en la empresa.* Observatorio Nacional de Tecnología y Sociedad, Red.es, Secretaría de Estado de Digitalización e Inteligencia Artificial. Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://www.ontsi.es/es/publicaciones/tecnologias-digitales-en-la-empresa-2023 [consulta: 15/7/2023].

El dato como recurso estratégico

En este contexto de digitalización, el dato pasa a convertirse en un valioso activo. Gracias a los datos es posible tomar decisiones de manera oportuna y segura, mejorar los procesos de producción, retener y atraer a más clientes, mejorar los productos o servicios y crear nuevos. No solo los datos estructurados o medibles resultan relevantes, sino que los datos no estructurados (imágenes, archivos audiovisuales, etcétera) también lo son, lo que pone aún más de manifiesto el potencial de las tecnologías basadas en ellos.

La conversión del dato en un recurso estratégico de primer orden ha intensificado el debate sobre la ética y la defensa de los derechos digitales, especialmente condicionado por el elevado valor que su posesión reviste para los depositarios de los contenidos. Dentro de estos parámetros, el debate sobre la ética del dato se acrecienta a medida que avanzamos de la inteligencia de datos al siguiente estadio tecnológico: la inteligencia artificial.

Soberanía digital y ética y derechos humanos

El derecho a la privacidad de los usuarios de servicios digitales ocupa un lugar central. El acceso seguro a los servicios públicos y privados en línea supone que los ciudadanos puedan proteger su identidad y controlar los datos que comparten y su utilización, de manera que se garantice su privacidad.

Disponer de una identidad digital segura es una pieza clave para la ciberseguridad. Uno de los grandes retos del mundo *online* es contar con mecanismos que permitan demostrar fehacientemente la identidad de una persona en el ámbito digital, esto es, que la persona natural o jurídica pueda acreditar fehacientemente su identidad para realizar una transacción o acceder a un servicio en línea. Surgen así los medios de identificación —decir quién se es— y autenticación —demostrar que se es quien se dice ser—, necesarios para utilizar la práctica totalidad de las plataformas y servicios en red y, en el ámbito de la empresa, para acceder a los sistemas de información.

En este sentido, la Estrategia Nacional de Inteligencia Artificial española (ENIA)[14] señala que el potencial impacto positivo del desarrollo y despliegue de la inteligencia artificial genera expectativas, pero también incertidumbres sobre sus implicaciones éticas, legales, sociales y económicas.

España está protagonizando el debate sobre los derechos digitales a nivel europeo y global. Entre otros avances, destaca la adopción por parte del país de la Carta de Derechos Digitales[15], un documento específico para asegurar los derechos constitucionales y el respeto a los derechos fundamentales de los ciudadanos en el entorno virtual y digital.

Con este bagaje, España ha liderado iniciativas importantes como la Declaración de Principios y Derechos Digitales de la Unión Europea[16], que, de forma explícita, sitúa a las personas como núcleo de la transformación digital de la UE. Además, la declaración señala que la tecnología debe servir y beneficiar a todas las personas y empoderarlas para que cumplan sus aspiraciones con total seguridad y sus derechos fundamentales se respeten plenamente.

Entre los desarrollos normativos que tratan de dar respuestas a esta materia se encuentra la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

El carácter central de la información personal tiene aspectos positivos porque permite nuevos y mejores servicios, productos o hallazgos científicos, pero también conlleva riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles para más actores y cada vez resultan más fáciles de procesar, mientras que es más difícil controlar su destino y uso.

[14] GOBIERNO DE ESPAÑA. Estrategia Nacional de Inteligencia Artificial. Noviembre de 2020. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf [consulta: 15/7/2023].
[15] GOBIERNO DE ESPAÑA. Carta de Derechos Digitales. 14 de julio de 2021. Disponible en: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210714_np_Carta-.aspx [consulta: 12/7/2023].
[16] UE. European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01). DOCE. 23 de enero de 2023. Disponible: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001 [consulta: 12/7/2023].

La tecnología desde la seguridad: oportunidad vs. desafío

Desde un punto de vista estratégico, los cambios sustanciales derivados de la innovación tecnológica en todos los niveles influyen de forma decidida en la conformación del nuevo sistema de seguridad global. En este sistema, se ha producido un cambio en la morfología de los riesgos y amenazas, y la tecnología se ha convertido en el elemento común.

En dicho contexto, existe una clara tensión en torno al control del conocimiento y de los desarrollos de tecnologías punteras dentro del escenario geopolítico global, lo que, asimismo, es relevante desde el punto de vista de la seguridad. La lucha por el liderazgo tecnológico entre EE. UU. y China es un claro ejemplo de ello.

La Estrategia de Seguridad Nacional 2022 de EE. UU.[17] aborda el ámbito tecnológico como motor de cambio y sustrato de su prosperidad económica y fortaleza militar, pero también como un entorno de competición geopolítica.

Por su parte, el último documento estratégico para la seguridad y la defensa de la UE[18], refrendado en el Consejo Europeo de marzo de 2022, no es ajeno a esta situación. En el capítulo relativo a las «Amenazas y desafíos emergentes y trasnacionales», se hace mención al uso de tecnologías emergentes y disruptivas por parte de actores estatales y no estatales que buscan alcanzar una ventaja estratégica y aumentar la eficacia de sus campañas híbridas. Al mismo tiempo, se aborda la vulnerabilidad que representa la dependencia de las tecnologías digitales, con lo que el ciberespacio se consolida como un terreno de competencia estratégica.

En España, la Estrategia de Seguridad Nacional 2021 (ESN 2021)[19], documento estratégico vertebrador de la política de seguridad del país[20], pone de manifiesto la trascendencia actual de la innovación tecnológica.

---

[17] THE WHITE HOUSE. National Security Strategy. 12 de octubre de 2022. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf [consulta: 15/7/2023].

[18] CONSEJO DE LA UNIÓN EUROPEA. A Strategic Compass for Security and Defence. 21 de marzo de 2022. Disponible en: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf [consulta: 19/7/2023].

[19] Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

[20] La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional establece en su artículo 4.1 que la política de seguridad nacional es «una política pública, en la que, bajo la dirección del presidente del Gobierno y la responsabilidad del Gobierno, participan todas las administraciones públicas, de acuerdo

En este sentido, la transformación digital se aborda como uno de los cuatro vectores de transformación del orden global, al igual que el contexto geopolítico, el entorno socioeconómico y la transición ecológica. Junto a todo ello, la ESN 2021 refleja cómo el desarrollo tecnológico amplía el espacio de exposición a nuevas amenazas, al tiempo que considera los riesgos asociados al uso de las nuevas tecnologías uno de los principales desafíos para la sociedad actual. Como contrapunto, enfatiza el papel en el ámbito de la seguridad de desarrollos basados en tecnologías emergentes, como la inteligencia artificial, para actuar frente a los desafíos globales.

Figura 5. Seguridad global y vectores de transformación de la seguridad global
Fuente: GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional 2021. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 [consulta: 19/7/2023].

Dimensión tecnológica de los riesgos y amenazas para la seguridad nacional

En el momento actual, tal como se refleja en la ESN 2021, la tecnología ha pasado a ser un factor común y destacado para todos y cada uno de los principales riesgos y amenazas a la seguridad nacional, con un mayor protagonismo en ámbitos como la vulnerabilidad del ciberespacio, la desinformación o las acciones de ciberespionaje. No obstante, su presencia también es significativa para amenazas relacionadas con la

con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional».

seguridad energética, la seguridad aeroespacial o la protección de las infraestructuras críticas.

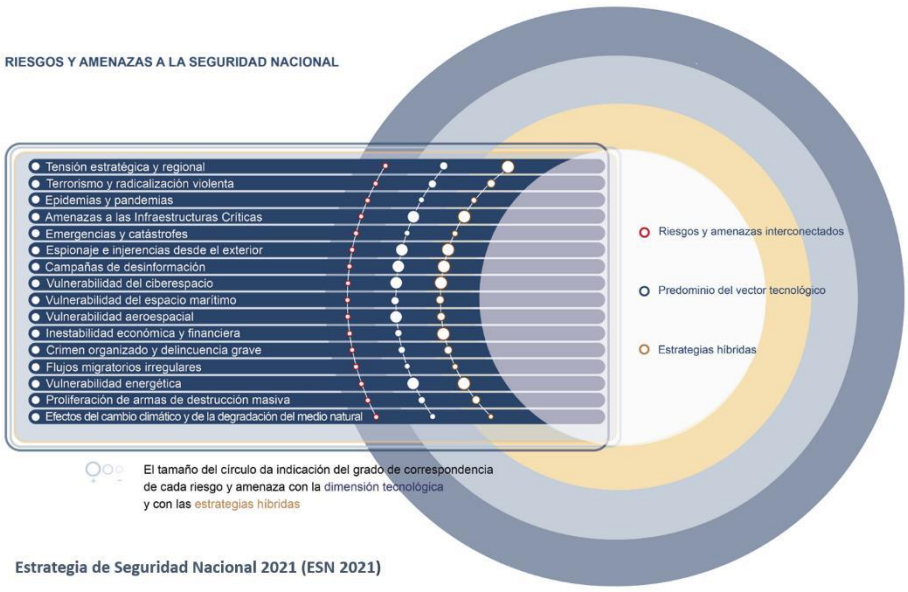

Figura 6. Riesgos y amenazas a la seguridad nacional
Fuente: GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional 2021. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021 [consulta: 19/7/2023].

Ante esta nueva morfología de los desafíos para la seguridad nacional, se han establecido distintas líneas de actuación: la tecnología y el impulso regulatorio de su uso cobran gran protagonismo en la prevención, preparación y respuesta eficaz ante contingencias que comprometan la seguridad y el bienestar de los ciudadanos.

A modo de ejemplo, y sin ánimo de exhaustividad, se expondrá brevemente la influencia de las tecnologías basadas en la inteligencia artificial sobre algunos de los riesgos y amenazas citados, entre los cuales este vector tiene una especial relevancia. Tal es el caso de las amenazas a las infraestructuras críticas, las posibles acciones de espionaje e injerencias desde el exterior o la amplificación de las campañas de desinformación[21].

[21] ANQUELA, P. (SOMOSIERRA TECH). Comunicación personal, 15 de junio de 2023.

Amenazas a las infraestructuras críticas

Las infraestructuras críticas son aquellas que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, la gestión y la vida ciudadana en general, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios básicos esenciales. Cabe destacar que estas dependen cada vez más de las tecnologías de la información. Por consiguiente, tal y como señala la normativa de referencia[22], «la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques».

El éxito en el rendimiento de los algoritmos de la inteligencia artificial depende en gran medida de que los datos sean precisos y confiables. Si los datos utilizados para entrenar los sistemas de inteligencia artificial se ven comprometidos o se manipulan de manera maliciosa, podrían producirse errores en los resultados que afectarían negativamente las operaciones de las infraestructuras críticas. La generación de datos maliciosos que se asemejan a los reales y se inyectan en sistemas críticos en producción es la principal amenaza en este terreno.

Por su parte, los sistemas de infraestructuras críticas —como la energía, el transporte o las comunicaciones— pueden ser vulnerables a ciberataques que automaticen la búsqueda de vulnerabilidades a través de algoritmos de inteligencia artificial. Los atacantes pueden utilizar estos algoritmos para industrializar el descubrimiento de debilidades en los sistemas de seguridad y lanzar ataques más sofisticados y difíciles de detectar. En especial, los algoritmos basados en el aprendizaje por refuerzo *(reinforcement learning)*[23] pueden aprender de la experiencia, mejorando en cada interacción la precisión de su ataque.

Asimismo, los avances en inteligencia artificial pueden facilitar el robo de información sensible. Los sistemas de inteligencia artificial pueden ser utilizados para automatizar la identificación de datos críticos y extraer información valiosa de las infraestructuras críticas, ya sean datos financieros, de seguridad o planes estratégicos.

[22] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [consulta: 12/7/2023].
[23] Rama del aprendizaje automatizado *(machine learning)* basada en el resultado (acierto/error) de las acciones del agente informático, es decir, en su propia experiencia.

La dependencia excesiva de la inteligencia artificial en las infraestructuras críticas también puede generar vulnerabilidades. Si los sistemas de infraestructuras críticas dependen en gran medida de su aplicación y experimentan fallos o interrupciones, podrían surgir problemas graves en la prestación de servicios esenciales. Por ello, la supervisión humana es siempre imprescindible en este tipo de instalaciones.

Acciones de espionaje e injerencias desde el exterior

Por otro lado, la gran capacidad de almacenamiento y la potencia de cálculo de los algoritmos basados en inteligencia artificial pueden ser utilizados para recopilar, analizar y procesar grandes cantidades de datos de forma rápida y eficiente. Sin duda, esto facilita una vigilancia masiva que permite a los actores disponer de capacidad para monitorear y rastrear las actividades de las personas a través de la recopilación de datos en línea, como los disponibles a través de las redes sociales, el correo electrónico o las comunicaciones telefónicas.

No obstante, los sistemas de seguridad basados en la inteligencia artificial, como el reconocimiento facial o la detección de intrusos, pueden ser eludidos utilizando técnicas conocidas como «antagónicas» o «adversarias» *(generative adversarial networks)*[24] en la tecnología de aprendizaje de datos. De esta forma, los actores maliciosos pueden manipular imágenes, sonidos u otros datos para evadir la detección y llevar a cabo actividades de espionaje sin ser detectados.

La inteligencia artificial también puede ser utilizada para obtener información confidencial de gobiernos, organizaciones o individuos. Los algoritmos pueden ser entrenados para identificar patrones y vulnerabilidades en los sistemas de seguridad y encontrar formas de acceder a datos protegidos. Esto incluye el robo de secretos comerciales, información estratégica y datos gubernamentales sensibles.

[24] Aquellas orientadas a la inteligencia artificial generativa, creadora de contenido a partir de la discriminación de modelos erróneos mediante la identificación.

Amplificación de las campañas de desinformación

La inteligencia artificial está acumulando una creciente influencia en la generación automática de desinformación, tanto a nivel privado como en el sector público.

El gran avance experimentado en los últimos años por las tecnologías de procesamiento del lenguaje natural (*natural language processing* o NLP) ha ocasionado nuevos riesgos que deben ser tenidos en cuenta.

Los algoritmos basados en NLP pueden generar contenidos de manera automatizada, entre los que se incluyen las noticias falsas. Por ejemplo, a partir del análisis de grandes cantidades de datos, estos algoritmos pueden aprender a producir textos que parecen auténticos, lo que dificulta que los usuarios y los sistemas de verificación de noticias detecten su falsedad.

Estos algoritmos también tienen capacidad para amplificar los contenidos falsos. Los utilizados en las redes sociales y otras plataformas en línea pueden priorizar y amplificar la difusión de contenido viral, incluidas las noticias falsas. Además, sobre la base de las preferencias y el comportamiento de los usuarios, pueden mostrarles contenidos similares, lo que conllevaría la formación filtros de información que determinan qué mostrar basándose en sus inclinaciones. Junto a ello, la inteligencia artificial se utiliza a menudo para crear perfiles falsos y bots en las redes sociales. Estas cuentas automatizadas pueden difundir y promover activamente noticias falsas, lo que genera un impacto mayor y amplifica su alcance.

Por último, la aplicación de esta tecnología puede complicar la detección de las noticias falsas. A medida que los algoritmos de generación de texto y manipulación de medios se vuelven más sofisticados, el esfuerzo requerido para desarrollar sistemas de verificación de noticias y técnicas de detección que identifiquen con precisión los contenidos falsos aumenta.

Conclusión

El siglo XXI viene determinado por la irrupción de una forma distinta de hacer las cosas: la tecnología y sus nuevas manifestaciones son las palancas de un cambio cuya columna vertebral es la transformación digital. Las empresas y el sector público están inmersos

en este proceso, conocedores de su trascendencia y de su potencial en términos de eficiencia, sostenibilidad y crecimiento.

En el contexto de oportunidad descrito no faltan los desafíos relacionados con el rápido desarrollo de las nuevas tecnologías. Estas hacen que los marcos regulatorios vayan en desventaja, exigen la protección del individuo ante nuevas amenazas a su identidad y privacidad y suponen la aparición de activos —el dato— con gran valor estratégico.

En este escenario la desigualdad también se mide según nuevos parámetros, como la disponibilidad de las redes, la accesibilidad a los servicios o la tenencia de habilidades digitales. Todo ello hace necesario que, a nivel global, las políticas hacia los países menos favorecidos se enfoquen en la cobertura de tales carencias para reducir las brechas que puedan tener un impacto negativo sobre la seguridad.

De la misma manera, el mapa de los riesgos y amenazas para la seguridad ha experimentado cambios. La tecnología es el elemento común a todos ellos, especialmente en los ámbitos donde su influencia está más presente.

Para evitar caer en la improvisación, la evaluación continua de las amenazas y la aplicación de estrategias transversales para hacerles frente se han convertido en una realidad en las sociedades avanzadas, como es el caso de España.

La colaboración del sector público y privado y la mayor regulación de los aspectos relacionados con el diseño y el desarrollo de las tecnologías emergentes desde la perspectiva de la seguridad son clave para reducir los riesgos y preservar los potenciales beneficios.

Junto a ello, los desarrollos de gran proyección, como los basados en la inteligencia artificial, están llamados a ser herramientas clave para la preservación de la seguridad, especialmente en ámbitos estratégicos como la ciberseguridad, la seguridad aeroespacial o la protección de infraestructuras críticas.

Lo expuesto precisa la adquisición de conocimientos y habilidades en materia digital no solo para la transformación de los diversos sectores, sino para la toma de conciencia sobre los riesgos y las actuaciones necesarias para evitar su materialización o, en su caso, limitar el impacto.

La protección del individuo y su seguridad son el objetivo final de las actuaciones en este campo y, para su consecución, se precisa de la corresponsabilidad de las personas. Para la alfabetización digital es imprescindible el desarrollo de programas informativos y formativos en todos los ámbitos, y la colaboración público-privada y de la sociedad civil han de ir de la mano.

Con todo, tal y como se señala en el marco del Sistema de Seguridad Nacional a propósito del desarrollo de la cultura de seguridad nacional: «Una sociedad conocedora de las amenazas y desafíos para la seguridad es una sociedad mejor preparada y con mayor capacidad de sobreponerse ante las crisis a las que tenga que enfrentarse. Una sociedad concienciada es, pues, más segura, robusta y resiliente»[25].

*Marian Soto Soriguera**
Analista

[25] GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional 2017. Disponible en: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf [consulta: 18/7/2023].