ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

89/2019 8 de octubre de 2019

Manuel R. Torres Soriano *

El futuro de la competición estratégica a través del ciberespacio

El futuro de la competición estratégica a través del ciberespacio

Resumen:

El propósito de este trabajo es analizar las principales incertidumbres sobre cómo evolucionará la rivalidad estratégica entre Estados a través del ciberespacio durante los próximos cinco años. Se abordan los siguientes debates: a) Los posibles desenlaces y el horizonte temporal de la carrera por la supremacía tecnológica en el ámbito de la Inteligencia Artificial. b) Hasta qué punto se seguirá contemplando la libertad empresarial y la iniciativa privada como el entorno ideal en el cual florece el avance científico, o si, por el contrario, se percibirá como una desventaja estratégica. c) Las ventajas y debilidades que tienen los sistemas políticos autoritarios a la hora de fomentar y capitalizar los procesos de innovación tecnológica. d) Las probabilidades de que la pugna por el poder y la conflictividad en el ciberespacio evolucione de manera progresiva, o a través de un acontecimiento transformador que reordene de manera instantánea las prioridades.

Palabras clave:

Internet, estrategia, ciberinteligencia, Inteligencia Artificial, autoritarismo político.

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

The future of strategic competition through cyberspace

Abstract:

This article analyses the main uncertainties about how strategic rivalry between states through cyberspace would evolve over the next five years. The following debates are addressed: a) The possible outcomes and time horizon of the race for technological supremacy in the field of Artificial Intelligence. b) To what extent will entrepreneurial freedom and private initiative continue to be viewed as the ideal environment in which scientific progress flourishes, or whether, on the contrary, it will be perceived as a strategic disadvantage c) The advantages and weaknesses of authoritarian political systems in promoting and capitalizing the technological innovation processes. d) The likelihood that the struggle for power and conflict in cyberspace will evolve progressively, or through a transformative event that instantly rearranges priorities.

Keywords:

Internet, strategy, cyberintelligence, Artificial Intelligence, political authoritarianism.

Cómo citar este documento:

TORRES SORIANO, Manuel R. *El futuro de la competición estratégica a través del ciberespacio*. Documento de Opinión IEEE 89/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción

La tecnología no solo es el instrumento del cual se valen los gobiernos para avanzar hacia unos objetivos que permanecen estables, sino que también tiene la capacidad de modificar las reglas de juego y la viabilidad de algunas metas. Esta es la razón por la que cualquier estrategia nacional de ciberseguridad no solo trata de orientar el comportamiento de un Estado en el presente, sino también debe intentar anticipar las grandes tendencias, para que la irrupción repentina de un escenario inesperado no la deje en una posición de vulnerabilidad.

Sin embargo, a la imposibilidad metafísica de predecir el futuro, se le añaden las dificultades propias de hacer prospectiva de carácter tecnológico. Uno de los errores más comunes (y difíciles de esquivar) es centrar nuestra atención en un número reducido de grandes avances tecnológicos en fase de maduración, y extrapolar nuestros intereses y comportamiento en un escenario donde se han materializado todas esas promesas. Resulta relativamente fácil imaginar cómo será nuestro mundo si dispusiéramos de vehículos plenamente autónomos, impresoras 3D capaces de fabricar diseños complejos en cualquier material, sistemas de inteligencia artificial de propósito general, etc. Sin embargo, el verdadero desafío es predecir la irrupción de toda otra serie de innovaciones colaterales que, a priori no se nos antojan tan espectaculares y complejas, pero que tienen una enorme capacidad para modificar el comportamiento de las personas y cómo interactúan entre ellas.

El gurú de la ciberseguridad Bruce Schneier, a la hora de hablar de nuestros límites a la hora de imaginar el futuro, suele mencionar un ilustrativo ejemplo[1] proveniente de la aclamada película *Blade Runner* (1982). Una obra de ciencia ficción que sitúa su trama en una versión distópica de la ciudad de Los Ángeles en el año 2019. Cuando los guionistas tuvieron que imaginar cómo sería un mundo situado a casi cuarenta años de distancia, no tuvieron problemas en contemplar vehículos voladores y robots humanoides tan perfectos que, en su apariencia y comportamiento, eran prácticamente indistinguibles de los humanos. Sin embargo, su visión del futuro en otros aspectos más cotidianos seguía anclada en el presente. Así, por ejemplo, en una determinada

[1] SCHNEIER Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,* New York, W. W. Norton & Company, 2018.

secuencia, el protagonista (un caza-robots interpretado por Harrison Ford) necesita efectuar una llamada telefónica. Los responsables de la película predijeron con acierto que, en un futuro tan sofisticado tecnológicamente, esta comunicación se efectuaría en forma de video-llamada donde los interesados podrían disfrutar de una imagen nítida de su interlocutor. Sin embargo, no llegaron a imaginar que este no sería el único aspecto que se vería transformado en el ritual de las llamadas telefónicas. Por el contrario, en esta futurista película podamos ver al protagonista haciendo una llamada de la misma manera que lo hacía cualquier persona en la década de los ochenta: buscando un teléfono público adosado a la pared de un bar, marcando en un teclado físico un número anotado en un papel que llevaba en su billetera, e introduciendo monedas para que el teléfono funcionase.

El fallo de imaginación consiste en ignorar que, con carácter previo a la irrupción de las grandes innovaciones que pueden marcar un punto de inflexión, el desarrollo tecnológico ha hecho posible otra serie de desarrollos mucho menos exigentes tecnológicamente, pero que pueden ser incluso más poderosos a la hora de transformar la realidad. Convertir, por ejemplo, a los terminales telefónicos en un dispositivo de tamaño reducido que, no solo se puede transportar, sino que integra funciones propias de herramientas distintas como ordenadores, cámaras de fotos y sistemas de geolocalización, a priori no parece una revolución capaz de transformar la historia de la humanidad. Sin embargo, en su adopción por parte de la sociedad, se ha convertido en una pieza esencial para entender ámbitos tan distintos como la participación política, el comercio, el ocio, e incluso la forma que adoptan las relaciones de amistad, afectivas y sexuales.

Cuando predecimos el futuro, tal y como señala el futurólogo Roy Amara, no solo tendemos a sobreestimar los efectos y la velocidad del cambio tecnológico en el corto plazo, sino que ignoramos sistemáticamente el poder acumulativo de las mejoras graduales en tecnologías existentes, las cuales pueden alcanzar un punto disruptivo del que casi nadie se había percatado. En este sentido, el potencial revolucionario de la Inteligencia Artificial durante los próximos años consiste en añadir un nivel de mejora a múltiples tecnologías existentes, las cuales, gracias a ese suplemento, se verán convertidas en herramientas sustancialmente distintas a las que ya conocíamos. Uno de los fundadores de *Wired*, la revista de referencia sobre tecnología, lo describía así: «La IA ya está aquí, es real, se está acelerando...la fórmula para las próximas 10 000

nuevas empresas de Silicon Valley es tomar algo que ya existe y añadirle Inteligencia Artificial»[2].

Resulta relativamente fácil tratar de mapear las trayectorias actuales en el ámbito de la conflictividad entre Estados a través del ciberespacio si solo nos centramos en *the next bing think*, pero la realidad es que no tenemos ni idea de qué desarrollos intermedios terminarán condicionando esos escenarios. No existe nada parecido a un determinismo tecnológico que nos anticipe los efectos de estas innovaciones y cómo serán acogidas por la sociedad. Sin embargo, sí que podemos reflexionar sobre esas mismas incertidumbres y extraer algunas conclusiones para evitar «el shock del futuro»[3]. Tener un conocimiento aproximativo de las diferentes direcciones de la innovación tecnológica y su recepción por la sociedad permite sustentar alguna medida de anticipación, por modesta y limitada que esta pueda ser. No podemos evitar tener que navegar en aguas desconocidas, pero sí que podemos intentar portar con nosotros algún tipo de mapa de lo que podemos encontrar en nuestra travesía, aunque este plano sea imperfecto y deba ser sometido a una continua actualización.

A continuación, abordaré lo que considero son algunas de las principales incertidumbres sobre cómo evolucionará la rivalidad estratégica entre Estados a través del ciberespacio durante los próximos cinco años. Para ello no solo he centrado mi atención en los aspectos estrictamente tecnológicos sino, sobre todo, en cómo interactúan con otros factores procedentes del contexto político, social y cultural.

¿Cómo acabará la carrera por la supremacía tecnológica?

En el ámbito de la Inteligencia Artificial, las principales potencias se encuentran embarcadas en una carrera destinada a decidir quién se alzará con una posición dominante. Sin embargo, la determinación de los contendientes, el nivel de recursos

[2] MERRITT Jonathan. "Is AI a Threat to Christianity?", *Wired* (Feb 3, 2017), disponible en: https://www.theatlantic.com/technology/archive/2017/02/artificial-intelligence-christianity/515463/. Fecha de la consulta 12.9.2019.

[3] Esta expresión es el título de un popular libro escrito por el futurólogo Alvin Toffler en 1970. En esta obra, Toffler define el término shock del futuro como un estado psicológico provocado por "la desastrosa tensión y desorientación que provocamos en los individuos al obligarles a un cambio excesivo en un lapso de tiempo demasiado corto". Véase: TOFFLER Alvin. *El "Shock" del futuro*, Madrid, Plaza & Janes, 1995.

empleados y sus ventajas previas no tienen necesariamente que determinar quién será el vencedor, ni tampoco la forma que adoptará ese desenlace.

Existen, al menos, dos posibles alternativas. Por un lado, que, al igual que sucedió con la bomba atómica, algún actor sea capaz de capitalizar en un momento específico la maduración de una línea de investigación científica. En un escenario de este tipo, el Estado vencedor anunciaría al mundo dicho logro, con el objetivo de lanzar un mensaje disuasorio y asentar las bases del nuevo equilibrio de poder. Imaginemos, por ejemplo, que un Gobierno consiguiera hacerse con un ordenador cuántico plenamente funcional. La computación cuántica no solo permitiría hacer invulnerables sus sistemas e información frente a ciberataques implementados con computación convencional, sino, lo que es más importante, podría romper todas las contraseñas y sistemas de encriptación existentes, lo que le daría un poder omnisciente para acceder, procesar y explotar cualquier dato que no hubiese sido actualizado al nuevo paradigma tecnológico. Se rumorea que, durante años, distintos gobiernos han almacenado de manera sistemática datos encriptados de otras naciones con el objetivo de acceder a su contenido cuando la computación permita romper el cifrado. Esta explotación futura tiene múltiples utilidades como, por ejemplo, en el campo de la contra-inteligencia: rastreando espías extranjeros y sus fuentes[4]. Con el propósito de dificultar que otros países puedan tratar de minimizar los daños ocasionados por esta nueva situación de supremacía tecnológica, es posible que la potencia vencedora tratase de ocultar temporalmente este hito, al menos hasta que el desequilibrio sea obvio. La llegada de la computación cuántica podría provocar una «era de desnudez» donde todos los datos que gobiernos y ciudadanos han generado durante décadas bajo la falsa premisa de que mantenían el control sobre ellos, de manera repentina han quedado expuestos al escrutinio público. Resulta fácil imaginar el tipo de conmoción generalizada que provocaría una situación donde se ha eliminado de manera repentina cualquier espacio para la privacidad y la intimidad en nuestras vidas. Una situación traumática que terminaría incluso alterando el sistema de valores morales y las normas de conducta social.

[4] CLARKE Richard A & KNAKE Robert K. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats,* New York, Penguin Press, 2019.

Otra posibilidad es que, a diferencia de la carrera espacial, en el desarrollo de la IA no existirá un momento «llegada del hombre a la Luna» que describa de manera inequívoca quien ha resultado vencedor en esta pugna. Por el contrario, el desarrollo sería incrementalista y acumulativo, con múltiples hitos intermedios[5]: actualizaciones de algoritmos, parches de software, etc. Esta variante no implica necesariamente que esta carrera tecnológica se prolongue durante décadas, antes bien puede desenvolverse a un ritmo frenético como consecuencia de la extensión de la Ley de Moore al ámbito de la IA, lo que implica que en algún momento la curva de maduración de algunas tecnologías abandonará su velocidad lineal para subirse a una pendiente exponencial. Así, por ejemplo, retomando el ejemplo de la computación cuántica, la transición de un paradigma a otro no se produciría de manera sorpresiva, sino como consecuencia del paso escalonado entre unas capacidades de procesamiento (convencional) cada vez más asombrosas, y unas primeras computadoras cuánticas en estado embrionario, de las cuales no resultaría posible extraer todo su potencial implícito. Lejos de producirse un «tsunami cuántico» que termine arrasando con el control sobre nuestros datos, se producirá una reacción de anticipación similar a la que se dio en el mundo de la informática con el llamado «efecto 2000»[6] cuyos daños terminarían siendo marginales. El carácter progresivo de la innovación tecnológica también es coherente con la naturaleza de la investigación científica contemporánea, la cual es lo suficientemente compleja como para que ningún centro de investigación o empresa tenga la capacidad de abordar en solitario todos los pasos necesarios para hacer operativo un avance científico. Por el contrario, el tejido científico se encuentra atomizado en miles de unidades desperdigadas en decenas de países, las cuales se encuentran a su vez interrelacionadas entre ellas y sometidas a una profunda movilidad de su personal. No solo será cada vez más difícil etiquetar con banderas nacionales las revoluciones

[5] CLIFFORD Jonathan. “AI Will Change War, But Not in the Way You Think”, War on the Rocks (September 2, 2019), disponible en: https://warontherocks.com/2019/09/ai-will-change-war-but-not-in-the-way-you-think/ Fecha de la consulta 12.9.2019.

[6] El “efecto 2000”, o también denominado Y2K en el ámbito anglosajón, consistió en un error común de diseño de software, causado por la falta de previsión de algunos programadores al omitir la centuria en el año para el almacenamiento de fechas (generalmente para economizar memoria), de tal manera que, tras finalizar el año 1999, estos programas reiniciarían la cuenta en el año 1900. Con anterioridad a la llegada del año 2000 existió una enorme preocupación por los efectos que este defecto podría generar en las redes informáticas que sustentaban servicios críticos, bancos, administraciones públicas, etc.

tecnológicas venideras, sino también que los distintos gobiernos puedan impedir su proliferación hacia otros países.

Globalización vs. proteccionismo tecnológico

El desarrollo de la IA y la robotización se han convertido en áreas donde el sector privado ha eclipsado a la inversión pública en I+D+i. Esta brecha entre gasto público y privado es enorme incluso con respecto a gobiernos que han decidido realizar una apuesta estratégica traducida en más gasto público. En el caso de Estados Unidos, se calcula que el montante anual del gasto del Departamento de Defensa para investigación en IA es menos de una décima parte de lo que dedican, de manera conjunta, cinco empresas ubicadas en el país: Google, Apple, Facebook, IBM, Microsoft y Amazon[7].

Los distintos gobiernos han asumido con naturalidad su papel gregario en esta carrera tecnológica, en la cual esperan que las empresas ubicadas en su territorio consigan liderar y transferir sus progresos al sector de la seguridad y la defensa. Esta sinergia entre sector empresarial y Estados, lejos de ser una novedad, ha resultado históricamente en una ventaja para los países que contaban con una vibrante iniciativa privada. En la actualidad, la naturaleza de esta relación es bastante más ambigua que la que tuvo lugar durante las grandes confrontaciones bélicas del pasado, donde las distintas empresas estaban plenamente alineadas con los esfuerzos bélicos de sus respectivos Estados.

Una de las novedades reside en que no existe un único marco de relaciones entre empresas y gobiernos, sino que en grandes rasgos el ecosistema de innovación tecnológica se ha dividido en dos grandes bloques. Por un lado, aquellas empresas que operan en un entorno de libre mercado, están internacionalizadas y toman sus decisiones con independencia de las preferencias gubernamentales. Y, por otro, aquellas empresas que, a pesar de operar en un mercado global, proceden de países donde se practica un

[7] DAVENPORT Thomas H. “China is overtaking the U.S. as the leader in artificial intelligence”, *Marker Watch* (March 7, 2019), disponible en: https://www.marketwatch.com/story/china-is-overtaking-the-us-as-the-leader-in-artificial-intelligence-2019-02-27 Fecha de la consulta 12.9.2019.

«capitalismo de Estado»[8] que legitima una profunda injerencia gubernamental en el funcionamiento y decisiones estratégicas de estas compañías.

Esta distinción es crucial para entender la rivalidad estratégica en el ciberespacio, ya que los éxitos privados no tienen por qué traducirse en una ventaja competitiva para el Estado en el cual se ubica legalmente la empresa. En los últimos años, hemos asistido a varios episodios que evidencian la voluntad de las principales compañías tecnológicas de reafirmar su plena independencia con respecto al sector gubernamental de sus respectivos países. Todas ellas son conscientes de que su implantación internacional puede resultar gravemente dañada si los consumidores de otros países asumen que esas marcas son una mera extensión de los intereses de terceros países. Sin embargo, en el caso de empresas chinas o rusas, las proclamas de independencia no dejan de ser meras operaciones de relaciones públicas, las cuales no invalidan el hecho de que, en última instancia, la matriz de dichas empresas está sometida a la arbitrariedad de unos Estados que pueden impedir la actividad de cualquier actor que no se pliegue a sus demandas. Por el contrario, en el bloque de las democracias liberales, la decisión de una empresa que no desee plegarse a su gobierno está amparada por un sistema efectivo de tutela judicial, el cual puede frustrar los intentos del Estado de alinear estas empresas con sus intereses estratégicos. Este es el caso, por ejemplo, del anuncio en 2018 por parte de Google de no renovar su contrato con el llamado Proyecto Maven del Departamento de Defensa de los Estados Unidos, un programa de inteligencia artificial destinado a analizar imágenes de vigilancia de vehículos aéreos no tripulados. Este contrato originó la protesta de 4 000 empleados de Google, los cuales mostraron reservas morales a participar en el desarrollo de lo que consideraban era un arma de guerra[9]. Este tipo de episodios pueden ser solo el principio de la desafección creciente entre empresas privadas y gobiernos. La adscripción nacional de los gigantes tecnológicos en el ámbito occidental tiende a difuminarse a medida que estas empresas se adaptan a la idiosincrasia de los mercados extranjeros, tienen una plantilla cada vez más internacionalizada y adquieren un volumen y relevancia que les permitiría, sin

[8] BREMMER Ian, “State Capitalism Comes of Age: The End of the Free Market?” *Foreign Affairs* Vol. 88, No. 3 (2009), pp. 40-55.

[9] THE ECONOMIST. “Artificial intelligence is changing every aspect of war”, *The Economist* (September 7, 2019), disponible en: https://www.economist.com/science-and-technology/2019/09/07/artificial-intelligence-is-changing-every-aspect-of-war.Fecha de la consulta 12.9.2019.

asumir un excesivo coste, deslocalizar su matriz y ubicarse en otro país que no imponga trabas y servidumbres. Frente a la creciente independencia de estos actores, los Estados solo pueden tratar de cultivar y agasajar al sector empresarial, sobre todo en la medida en que la coacción legal es cada vez menos efectiva y la compensación económica a través de contratos públicos queda eclipsada frente a las colosales ganancias que aporta un mercado global. En este escenario, el hecho de que una empresa estadounidense alcance la primacía en un determinado desarrollo tecnológico no tiene por qué traducirse directamente en una ventaja privativa para su país. Por el contrario, puede ser un tercer Estado el que termine capitalizando esa innovación a través de su adquisición en el mercado abierto.

Una de las principales incertidumbres consistirá en saber hasta cuándo seguirá contemplándose la libertad empresarial y la iniciativa privada como el entorno ideal en el cual florece la innovación, o si, por el contrario, se percibirá como una desventaja estratégica. Se abren dos posibles escenarios. Por un lado, que gane peso la postura que señala que la apertura comercial hacia empresas tecnológicas procedentes de países donde se practica un capitalismo de Estado supone una vulnerabilidad intolerable. Si en los próximos años se siguen produciendo episodios[10] donde se visualiza que los riesgos de la inserción de malware, puertas traseras y otro tipo de accesos no legítimos en las importaciones tecnológicas, lejos de ser una posibilidad teórica, se convierten en evidencias tangibles, es muy probable que se produzca una oleada de proteccionismo comercial basado en argumentos de seguridad nacional. La desglobalización iniciada por la presidencia de Donald Trump con el objetivo de proteger su industria manufacturera y contentar a los sectores obreros del país puede verse profundizada y asumida por otros países con el argumento de que entorpecer las importaciones tecnológicas de terceros y «balcanizar»[11] la gestión de internet es una forma de defender al país frente a sus enemigos. La innovación tecnológica se contemplará como un proceso donde deben primar las cuestiones de seguridad, aunque eso suponga asumir unos elevados costes

[10] ROBERSTON Jordan & RILEY Michael. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”, *Bloomberg Businessweek*, (October 4, 2018), disponible en: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies Fecha de la consulta 12.9.2019.

[11] SCOTT Mark. “Goodbye internet: How regional divides upended the world wide web”, *Politico*, (January 18, 2018), disponible en: https://www.politico.eu/article/internet-governance-facebook-google-splinternet-europe-net-neutrality-data-protection-privacy-united-states-u-s/ Fecha de la consulta 12.9.2019.

económicos y de oportunidad. En este escenario, las grandes empresas internacionales se verían forzadas a convertirse en «campeones nacionales» cuyo destino está inevitablemente vinculado a los intereses estratégicos del país en el cual operan.

Sin embargo, esta transformación de la estructura comercial internacional no es inevitable. Resulta tremendamente complicado revertir un sistema productivo que está profundamente imbricado en la economía de múltiples países. La mayoría de Estados no tendrán la opción de optar entre unos productos nacionales (inexistentes o ineficaces) frente a desarrollos de otros países. Seguirán dependiendo de estas importaciones si no quieren quedarse descolgados de determinados avances clave que les permiten seguir siendo competitivos. Los gobiernos tendrán que aceptar resignados que no tienen otra opción distinta a la de aceptar los riesgos potenciales de sustentar sus infraestructuras críticas y sistemas de defensa en desarrollos que potencialmente pueden ser controlados y manipulados por terceros Estados. Esta dependencia no resultará tan difícil de sobrellevar si no se produce un escenario abierto de confrontación. En tiempos de competición, ninguno de los países que pueden ejercen ese control subrepticio tiene incentivos para hacer ostentación de un recurso que resulta mucho más útil si se mantiene discretamente en el arsenal. Ante la ausencia de un evento transformador que sacude las conciencias, será complicado que las élites políticas y militares sean capaces de transmitir a la sociedad el relato de los riesgos de la subordinación tecnológica. Sobre todo, cuando revertir esa situación implica un coste económico y pérdida de capacidad adquisitiva para una ciudadanía predispuesta a castigar electoralmente a los gobiernos que exigen sacrificios para una causa tan poco atractiva como la resiliencia frente a un hipotético conflicto.

¿Dilema del dictador o dilema del demócrata?

Durante décadas las relaciones económicas entre el bloque de países democráticos y los países con regímenes políticos autoritarios se han basado en la teoría de la modernización, según la cual, la mejor forma de apoyar la democratización de estos países era abrirlos al comercio internacional. La aceptación de las reglas del mercado, no solo convertiría a estos gobiernos en actores más previsibles y abiertos al compromiso, sino que también moderaría sus actitudes violentas y represivas. En paralelo, la participación en los mercados y el crecimiento económico terminaría

transformando progresivamente la estructura social de estos países, dando lugar a a emergencia de una nueva clase media más educada, activa políticamente y dispuesta a exigir una mayor rendición de cuentas a sus gobernantes. La idea de que la apertura comercial y la liberalización política se apoyan mutuamente[12] permitió forjar metáforas como la del «dilema del dictador», según la cual, los autócratas tenían que enfrentarse a un dilema existencial: si quería participar en los beneficios y la riqueza que proporciona el comercio internacional tendrían que rebajar el nivel de control y represión que ejercen sobre la sociedad, permitiendo la iniciativa privada, la circulación de personas y los flujo de información. A medida que el país se hiciese más próspero se irían socavando las bases que permiten ejercer la autoridad política sin participación de los ciudadanos. La otra alternativa era mantener su férreo control sobre la sociedad, cerrando el país alos flujos económicos y de información, lo cual le mantendría en el poder, pero su país sería cada vez más pobre e irrelevante.

La espectacular transformación experimentada por China en las últimas décadas nos demuestra que el dilema del dictador es una simplificación que no ha conseguido atrapar la complejidad del cambio social y político en este país. Si bien queda poco en la estructura económica comunista, su élite política ha conseguido sumarse a los beneficios de participar en la economía global, sin que el control político sobre la sociedad se haya visto sustancialmente debilitado. La narrativa sobre la incapacidad de China para innovar, limitándose a robar y copiar los desarrollos de otros países, es anticuada y subestima su creciente pujanza tecnológica, la escala de sus inversiones y la tendencia a la planificación en el largo plazo[13]. Su habilidad para saber sortear las contradicciones entre las bases teóricas de su control político y la realidad social y económica de su país, se ha producido incluso con la irrupción de internet, una herramienta que algunos estimaron que haría imposible que el régimen comunista pudiese sobrevivir[14]. Los jerarcas chinos han demostrado que, con respecto a internet, no es necesario tomar la

[12] TORRES Manuel R. "Globalización, integración y regionalización política" en SZMOLKA Inmaculada (Ed.) *Elementos para el análisis comparado y procesos políticos*, Granada, Editorial de la Universidad de Granada, 2012, pp. 239-252.

[13] KANIA Elsa B. & COSTELLO John. “Quantum Hegemony? China’s Ambitions and the Challenge to U.S. Innovation Leadership”, *Center for a New American Security*, (September 12, 2018), disponible en: https://www.cnas.org/publications/reports/quantum-hegemony Fecha de la consulta 12.9.2019.

[14] TORRES Manuel R. "Internet como motor del cambio político: ciberoptimistas y ciberpesimistas", *Revista del Instituto Español de Estudios Estratégicos*, Nº1 (2013), pp. 127- 148.

decisión dicotómica de abrazarlo en su integridad o cerrar la sociedad al ciberespacio, sino que existen formas mucho más sutiles[15] de ejercer un control efectivo sobre aquellos usos de internet que pueden suponer una amenaza a su continuidad en el poder.

Si relacionamos este debate con nuestra reflexión sobre el futuro de la competición estratégica encontramos una paradoja: la actual estructura política y social de China, lejos de suponer un problema, puede ser un potenciador de sus capacidades frente a sus competidores en el bloque democrático. Pensemos, por ejemplo, en el desarrollo de sistemas basados en *machine learning*. La sofisticación y eficacia de estos sistemas de aprendizaje autónomo se basa en la calidad y cantidad de los datos que utiliza para extraer patrones. En este proceso, China tiene dos ventajas fundamentales: un gobierno autoritario y la cuarta parte de la población mundial. Cuando el objetivo de liderar la carrera tecnológica está muy por encima de cualquier preocupación sobre el respeto a los derechos individuales y la privacidad de sus ciudadanos, China puede hacer cosas que otros países ni siquiera llegarían a plantearse. Su población se convierte al mismo tiempo en el combustible que alimenta de datos a estos sistemas de aprendizaje automático y en el destinatario de estas aplicaciones que contribuyen a reforzar el control político y eliminar a la disidencia. Los marcos normativos, lejos de suponer un freno a la voracidad de unos sistemas que necesitan penetrar en la intimidad de los usuarios, son puestos al servicio de la mejora de la eficiencia de estas aplicaciones. China está siendo pionera en la adaptación de herramientas cuyas implicaciones éticas resultan paralizantes en otras latitudes[16]: desde la imputación de delitos a través de sistemas de policía predictiva, a la implantación de sistemas de crédito social, donde un algoritmo determina quiénes son los ciudadanos ejemplares que deben ser premiados y cuáles deben ser marginados. Con esta capacidad de experimentación en situaciones reales, resulta altamente probable que, en los próximos años, China sea la campeona indiscutible en el desarrollo de cualquier plataforma cuya sofisticación necesite cantidades masivas de datos. A la falta de límites en la injerencia del poder político sobre la vida de los ciudadanos, se suma una cuestión de magnitud. En el mercado chino,

[15] MACKINNON Rebecca. "Liberation Technology: China's "Networked Authoritarianism", *Journal of Democracy*, Vol. 22, No. 2 (2011), pp. 32-46.

[16] LARSON Christina, “Who needs democracy when you have data?”, *MIT Technology Review*, (August 20, 2018), disponible en: https://www.technologyreview.com/s/611815/who-needs-democracy-when-you-have-data/ Fecha de la consulta 12.9.2019.

cualquier innovación tecnológica tiene garantizada (tanto de manera voluntaria, como coactiva) la mayor fuente de datos del planeta. No es accidental que los mayores éxitos empresariales de la era de la información (Google, Facebook, Amazon, Alibaba, etc.) sean prácticamente monopolistas en sus sectores de mercado. Cuando hablamos del acceso a los datos existe un círculo virtuoso: más y mejores datos permiten a las compañías ofrecer mejores servicios y aplicaciones, lo que aumenta sus ingresos y popularidad, lo que a su vez se convierte en más datos, y en la práctica expulsión de ese sector de aquellos competidores que no cuentan con el acceso a esos volúmenes de información. Esa realidad comercial puede trasladarse al ámbito de la rivalidad geopolítica[17], donde existen potencias que están convencidas que se encuentras embarcadas en una carrera excluyente, donde el primero en llegar podrá ejercer una hegemonía sobre el resto. En un sorprendente giro de la historia, el tamaño de la población de un país vuelve a ser un indicador esencial de su poder. Pero, a diferencia de lo que sucedía en las grandes guerras, los hombres no son valiosos porque pueden ser convertidos en soldados, sino por su utilidad para producir los datos que alimentan los algoritmos que librarán las batallas del futuro.

¿Evolución progresiva o cambio dramático?

Los grandes procesos de cambio político y social no se desarrollan de manera lineal. Su despliegue está repleto de continuas oscilaciones que explican el ritmo y la intensidad con la que son adoptados por la sociedad. En ocasiones estas perturbaciones adquieren la forma de un verdadero cataclismo que permite dibujar claramente el momento exacto en el que se produce un antes y un después en la historia (ej. el ataque a Pearl Harbor, el bombardeo de Hiroshima y Nagasaki, la caída del muro de Berlín, los atentados del 11S, etc.) La forma en la que se desarrolle la pugna por el poder y la conflictividad en el ciberespacio también es susceptible de evolucionar por una de estas dos vías: de manera progresiva y continuada, o través de un acontecimiento transformador que reordene de manera instantánea todas las prioridades.

[17] ROSENBACH Eric & MANSTED Katherine,"The Geopolitics of Information*", Belfer Center for Science and International Affairs* (May 28, 2019), disponible en: https://www.belfercenter.org/publication/geopolitics-information Fecha de la consulta 12.9.2019.

A favor de la hipótesis del cambio dramático encontramos un amplio conjunto de factores de riesgo. Por un lado, se ha asumido el marco narrativo de que nos encontramos en una carrera entre potencias. Cuando la prioridad absoluta es ser el primero en alcanzar algunos de los hitos de esta competición, el efecto es que las cuestiones relacionadas con la seguridad y fiabilidad de estos avances científicos quedan relegadas a un segundo plano. El verdadero peligro de una carrera armamentista no es que gane tu enemigo, sino que todos los participantes pierdan por haber adoptado tecnologías inseguras que terminan provocando un daño generalizado.

Los sistemas de Inteligencia Artificial basados en el aprendizaje profundo pueden ser inescrutables. Los investigadores a menudo son incapaces de entender cuál es la lógica que guía el comportamiento de un sistema que ha interiorizado por sí mismo una serie de patrones extraídos del consumo masivo de datos. Podemos entender que está haciendo, pero no por qué lo hace, lo que lo convierte en un comportamiento impredecible. Testar los sistemas basados en IA puede llevar aún más tiempo y dinero que probar el hardware militar convencional[18]. Su complejidad es la clave que los convierte en herramientas muy poderosas pero, al mismo tiempo, aumenta la probabilidad de problemas inesperados. Pensemos, por ejemplo, en la posibilidad de que un gobierno desarrollara un sistema de IA que pudiera, de manera autónoma, penetrar y tomar el control de la totalidad de las redes informáticas de sus adversarios evitando la detección. El primer gobierno que consiguiera desplegarlo adquiriría una posición de ventaja muy difícil de revertir. Preocupados por el hecho de que un adversario esté desarrollando una herramienta similar, los gobiernos podrían sentirse obligados a interrumpir las pruebas y ser los primeros en utilizar este sistema. Este no sería el primer caso en el que un gobierno confía en una tecnología poderosa, pero insegura. En el contexto de la Guerra Fría, el despliegue de las primeras redes informáticas en el ámbito militar buscaba aumentar la velocidad y la capacidad de respuesta de sistemas críticos, en un momento donde se contemplaba como una amenaza real la posibilidad de sufrir un ataque nuclear sorpresivo. Sin embargo, la urgencia obligó a subestimar las numerosas vulnerabilidades estructurales de estas primeras redes, algunas de las cuales seguimos padeciendo en la actualidad.

[18] SCHARRE Paul, “Killer Apps. The Real Dangers of an AI Arms Race”, *Foreign Affairs*, (May/June 2019), disponible en: https://www.foreignaffairs.com/articles/2019-04-16/killer-apps Fecha de la consulta 12.9.2019.

El panorama no es mucho más alentador en el sector privado. A lo largo de los últimos años, hemos asistido a un verdadero torrente de escándalos donde, compañía tras compañía, han sufrido importantes filtraciones de datos provocadas por una gestión negligente de la seguridad de sus propios sistemas. Sin embargo, ninguno de estos incidentes ha supuesto un deterioro de su posición en el mercado, incluso en aquellos casos donde estas empresas han ocultado deliberadamente estos incidentes durante años. Teniendo en cuenta que el precio de las acciones de las empresas irresponsables no se ve afectado en el largo plazo, estas tienen fuertes incentivos para tratar los incidentes de ciberseguridad como un mero problema de relaciones públicas. Este es un escenario que se parece demasiado a lo que los economistas llaman un «mercado de limones»[19]. Las compañías solo compiten por características que los consumidores pueden identificar, e ignoran otras características (como la ciberseguridad) que resultan más complejas de percibir por parte del consumidor. Los productos inseguros terminan desplazando del mercado a los seguros, porque la inversión en ciberseguridad apenas produce retornos en el corto plazo[20]. Un mundo repleto de sistemas de Inteligencia Artificial desprotegidos no es solo una posibilidad, sino que puede ser la configuración predeterminada.

Este evento transformador también puede estar sustentado en la creciente capacidad de procesar y capitalizar las numerosas filtraciones de datos que se han producido en los últimos años. Muchas de las noticias publicadas sobre el robo de bases de datos que incluyen millones de contraseñas, datos personales, información financiera, historial médicos, correos electrónicos, etc., generan una breve alarma social, pero los ciudadanos no perciben que el acceso ilegítimo a sus datos se vea materializado en una acción que les pueda perjudicar en el «mundo real». Rob Joyce, el primer coordinador de ciberseguridad nombrado por el presidente Donald Trump, declaró, por ejemplo, que su número de seguridad social había sido robado hasta en seis ocasiones distintas en

[19] "The Market for 'Lemons'" es un artículo escrito por George Akerlof en 1970, cuyo objetivo es explicar algunos de los fallos de mercado derivados de la información imperfecta. El trabajo utiliza el ejemplo de alguien que quiere comprar un coche de segunda mano. El mercado se compone de dos tipos de coches: los que se venden de buena fe y los que se están vendiendo por ser poco fiables: estos son los llamados "limones" (en el argot estadounidense). Véase: AKERLOF George A. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", *The Quarterly Journal of Economics*, Vol. 84, No. 3 (1970), pp. 488-500.

[20] SCHNEIER Bruce. Ob. Cit. Nota 1.

diferentes filtraciones de datos[21]. Sin embargo, esto puede cambiar muy rápidamente. Hasta el momento, el principal factor que ha protegido a las víctimas de este robo de información ha sido precisamente que sus datos personales estaban difuminados en un auténtico océano de información, cuyo análisis y explotación indiscriminada resultaba inasumible incluso para los actores gubernamentales. La sustitución del elemento humano por sistemas de explotación de datos basados en Inteligencia Artificial está haciendo posible que, por primera vez, sea rentable analizar individualizadamente cada una de las unidades de estas bases de datos. Los grupos dedicados a las ciberestafas o la persuasión política, por ejemplo, ya no tendrán necesidad de lanzar burdos mensajes fraudulentos a millones de internautas con la esperanza de que algunos de ellos piquen el anzuelo o se deje persuadir. La adaptación de estos mensajes a la idiosincrasia del destinatario, lo cual plantea un engaño mucho más sofisticado y difícil de detectar, será la obra de sistemas automatizados que son capaces de abarcar y extraer utilidad a la totalidad de los datos que se les proporcione. Pensemos, por ejemplo, en las consecuencias que tendría la explotación en el ámbito de una operación de inteligencia de los datos robados por actores chinos a la OPM (Oficina de Gestión de Personal de Estados Unidos), los cuales incluían nombres, fechas, lugares de nacimiento, comprobaciones de antecedentes de seguridad, datos sobre personal de inteligencia y militar, y los datos de huellas dactilares de 5,6 millones de empleados públicos estadounidenses. Los intrusos incluso accedieron al formulario de solicitud de autorización de seguridad, el cual incluye información como registros de uso de drogas, adicción al alcohol y problemas financieros. Este tipo de datos, no solo tienen un valor evidente para sustentar operaciones hostiles de espionaje basadas en el chantaje o la captación de fuentes humanas[22], sino que, si se combinan con los registros de esas mismas personas obtenidos en otro tipo de filtraciones de datos de empresas, bancos y redes sociales de Internet, permiten que un país extranjero pueda ejercer un enorme poder coactivo sobre la totalidad del elemento humano que sustenta un Estado. El hecho transformador puede ser, precisamente, que un actor decida hacer uso estratégico del

[21] CARLIN John P. & GRAFF Garrett M. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat,* New Yok, PublicAffairs, 2018.

[22] SMEETS Max, "There Are Too Many Red Lines in Cyberspace", *Lawfare* (March 20, 2019), disponible en: https://www.lawfareblog.com/there-are-too-many-red-lines-cyberspace Fecha de la consulta 12.9.2019.

potencial que encierran todos estos datos para condicionar el curso político de otro Estado, ejecutar una represalia, o plantear una extorsión.

No obstante, el fin de la ingenuidad no tiene necesariamente que producirse por un hecho espectacular que sirva como revulsivo para la mentalidad de gobiernos y personas. En otras ocasiones, las sociedades modifican el curso de determinadas tendencias a partir de pequeños cambios acumulativos. Pensemos, por ejemplo, en la seguridad en el transporte aéreo. La implantación de un estricto estándar de investigación sobre las causas de los accidentes y la incorporación obligatoria de las lecciones aprendidas en cada siniestro a todos los operadores ha terminado convirtiendo un hecho tan peligroso y complejo como volar, en el medio de transporte más seguro. La situación actual de ciberseguridad, aunque muy mejorable, es sustantivamente mejor que la que existía tan solo hace diez años. La experiencia acumulada ha dado lugar a actores mucho más sofisticados con una mayor concienciación sobre los riesgos que comporta el ciberespacio. Este aprendizaje progresivo ha terminado haciendo obsoletas determinadas prácticas ofensivas que, tan solo hace unos años, apenas encontraban resistencia. Quizás en un futuro cercano, y sin la necesidad de un cataclismo, el ciberespacio se convierta en territorio mucho fiable y seguro.

Conclusión: mirar hacia la política

El futuro de la competición estratégica en el ciberespacio no está condicionado únicamente por la tecnología. Los atributos del poder político y la naturaleza de los contendientes son variables fundamentales para entender cómo puede desenvolverse esta pugna. Las proyecciones futuras que prescinden de las variables políticas se fundamentan en una premisa errónea: que la innovación tecnológica tiene lugar de manera aislada. Sin embargo, la historia nos muestra cómo los actores políticos son los protagonistas fundamentales en estos procesos de cambio. Los Estados no solo asignan recursos y fijan objetivos, sino que, sobre todo, aportan el contexto que favorece o constriñe la innovación.

Integrar la variable política en la prospectiva tecnológica implica ir más allá de las categorías tradicionales que dividen el mundo entre dictaduras o democracias; mercados libres o intervenidos por el poder político; enemigos o aliados, etc. En las últimas décadas hemos tenido numerosos ejemplos de cómo la pugna política está teñida de numerosas tonalidades grises que desafían los marcos de análisis con los que habíamos contemplado el mundo.

China es un excelente ejemplo de este desafío intelectual que nos obliga a recurrir a categorías mucho más sutiles a la hora de reflexionar sobre el futuro. Pero también cometeríamos un error si prescindiésemos de cualquier lección que se fundamente en un precedente histórico. Los autoritarismos políticos tienen una enorme ventaja frente a las democracias a la hora de planificar en el largo plazo y seguir un cauca de acción coherente con sus objetivos. Esta es una de las causas fundamentales del espectacular ascenso del país asiático en las dos últimas décadas. Sin embargo, el crecimiento chino arrastra una vulnerabilidad fundamental que no afecta a los países democráticos: la legitimidad. El país vive en una contradicción flagrante entre los fundamentos ideológicos que sustentan su régimen político y su realidad socioeconómica. El comunismo es una ficción nominal, pero sigue siendo la razón que justifica que la sociedad esté apartada de la participación política y se vea sometida de manera coactiva por una pequeña élite bajo la forma de un partido único. Los jerarcas chinos han podido sortear esta contradicción legitimando el régimen en la eficacia económica. Mientras que el país ha ido creciendo de manera continuada y reduciendo drásticamente la pobreza, estas han sido cuestiones que han quedado relegadas entre una sociedad despolitizada, cuya principal aspiración es seguir mejorando su calidad de vida. Sin embargo, ninguna sociedad en la historia ha sido capaz de crecer sin experimentar de manera cíclica crisis económicas que vapulean los pilares del orden social. China no será una excepción. Es más, tiene un peor pronóstico a la hora de afrontar algunos de los principales desafíos de los próximos años. Así, por ejemplo, si en Occidente causa temor cómo encarar la próxima extinción de empleo provocada por la robotización de la economía, en el caso de China, esto puede provocar un cataclismo social imposible de digerir por un régimen cuya supervivencia depende de un crecimiento infinito.

*Manuel R. Torres Soriano**
Profesor Titular de Ciencia Política, Universidad Pablo Olavide de Sevilla
Miembro del Grupo de Estudios en Seguridad Internacional (GESI)