Es necesario tomar medidas no solo para regular las tecnologías emergentes, sino también para entender y abordar las vulnerabilidades de nuestro sistema cognitivo que puedan ser objeto de ataque

La guerra cognitiva convierte la mente en un campo de batalla

Irene Pujol
Centro para la Gobernanza del Cambio de IE University

EN una era marcada por tensiones geopolíticas, avances tecnológicos sin precedentes y cambios disruptivos, se abre un nuevo campo de batalla: la mente. La «guerra cognitiva», un concepto que el *Innovation Hub* de la OTAN lleva estudiando desde 2021, supone un punto de inflexión en los conflictos a escala global al convertir en un objetivo estratégico el control de la cognición humana. De hecho, la guerra cognitiva presenta una creciente amenaza de seguridad global, impulsada por el progreso de la neurociencia, la inteligencia artificial y otras tecnologías emergentes, así como la proliferación de las redes sociales. Resulta, pues, crucial entender esta amenaza en constante evolución y prepararse para hacerle frente.

Si bien a lo largo de la historia las operaciones de manipulación y engaño han formado parte de la táctica militar, el concepto de guerra cognitiva hace alusión a un cambio sustancial: el objetivo de influir en la forma de pensar, reaccionar y tomar decisiones de las personas y los grupos ha pasado de táctico a estratégico —un fin en sí mismo— y es cada vez más fácil de lograr. Dicho cambio se explica a partir de tres factores: mayor conocimiento, incentivos y medios para influir en la forma de pensar de los ciudadanos.

El factor «conocimiento» de la guerra cognitiva, que suele pasarse por alto, surge de nuestra creciente comprensión acerca de cómo funciona el cerebro humano tras décadas de investigación en los ámbitos de la neurociencia, la economía conductual y la psicología. En este sentido, según Gerald Zaltman, profesor de *Harvard Business School*, solo una mínima parte de nuestras decisiones —alrededor del 5 por 100— son racionales. El resto de ellas se ven condicionadas por lo que Herbert Simon llama racionalidad limitada y están influidas por factores inconscientes como la repetición, las respuestas automáticas, los sesgos y las falacias.

Como sostiene el premio nobel Daniel Kahneman en su libro *Pensar rápido, pensar despacio*, nuestro cerebro está programado para tomar atajos en la mayoría de las decisiones del día a día, como elegir qué comemos o cómo reaccionamos a las señales sociales; y esto es así porque tomar decisiones de manera racional consume mucha energía mental. Algunos de estos atajos mentales son: El efecto de anclaje (la tendencia a confiar excesivamente en la

Ofrece una forma de alcanzar objetivos estratégicos sin los riesgos y gastos asociados a la acción militar convencional

primera información que nos dan —el «ancla»— a la hora de tomar decisiones); o el sesgo de confirmación (la inclinación a buscar, interpretar y recordar información que confirma nuestras creencias e ideas preconcebidas).

Que alguien intente aprovecharse de nuestros sesgos cognitivos no es nada nuevo. Las empresas de marketing llevan años haciéndolo para hacernos creer que necesitamos sus productos (aunque, a menudo, no lo hagamos). Sin embargo, en la última década, el uso de nuestros sesgos cognitivos ha ido mucho más allá de manipular a los consumidores. Hoy en día, las campañas de desinformación y otras operaciones de influencia se han convertido en elementos centrales tanto de la política como de la guerra a nivel nacional e internacional.

¿Por qué? Porque existen incentivos para que así sea, el mencionado segundo factor detrás de la guerra cognitiva. La guerra cognitiva ofrece una forma segura y rentable de alcanzar objetivos estratégicos, a menudo sin los riesgos y gastos asociados a la acción militar convencional. Un ejemplo de este enfoque es la estrategia del ejército chino conocida como «guerra inteligentizada» contra Taiwán. Mediante el uso de técnicas de guerra cognitiva, China pretende controlar el destino de Taiwán sin recurrir a la guerra convencional, un planteamiento motivado en parte por la preocupación por la sostenibilidad del crecimiento económico chino.

Sin embargo, incluso en lugares de guerra activa y cinética, la gestión de la narrativa —que requiere una buena comprensión de cómo funciona la mente— se ha vuelto cada vez más crítica para «ganar la guerra». La actual guerra en Ucrania ilustra este punto. En un momento en que se necesita desesperadamente la acción de los gobiernos occidentales para cambiar el equilibrio militar contra la invasión rusa, las campañas rusas de desinformación para socavar el apoyo a Ucrania siguen intensificándose. Por ejemplo, Ralf Beste, jefe del departamento de cultura y comunicación del Ministerio Federal de Asuntos Exteriores de Alemania, declaró al *Financial Times* que su equipo había identificado este año una red de más de 50.000 cuentas falsas que generaban hasta 200.000 mensajes diarios. Su objetivo era persuadir a los alemanes de que el apoyo del gobierno a Ucrania pone en peligro la prosperidad alemana y aumenta el riesgo de guerra nuclear «identificando dudas y sentimientos de malestar existentes e intentando agrandarlas». Aunque este tipo de estrategias y técnicas han sido habituales tanto en contextos de paz como de guerra durante décadas, su eficacia ha aumentado —y seguirá aumentando— debido a las innovaciones tecnológicas de las que estamos siendo testigos. Éstas proporcionan los medios para emprender una guerra cognitiva de amplio alcance e impacto.

El escándalo de *Cambridge Analytica* demostró cómo los datos de las redes sociales pueden explotarse para elaborar perfiles

psicológicos con fines de *microtargeting* político. En los últimos años, también hemos sido testigos del uso estratégico de cuentas falsas, *bots*, *influencers* digitales y la distribución de ***fake*** *news* a través de aplicaciones de mensajería como *Telegram* para avivar las tensiones raciales en Estados Unidos, promover golpes militares en el Sahel e impulsar la influencia de China en el extranjero. Sin embargo, pese a ser disruptivas, las campañas tradicionales de desinformación en las redes sociales han obtenido hasta la fecha resultados ambiguos en la consecución de objetivos estratégicos.

La IA generativa revolucionará este panorama. No solo aumentará el volumen y el alcance de las campañas de desinformación y otras operaciones de influencia al reducir las barreras financieras y técnicas a la creación de contenidos, sino que mejorará su calidad y eficacia. La creciente sofisticación de los *deepfakes* y otros contenidos generados por IA hará que a la gente le resulte más difícil distinguir lo que es real de lo que no lo es. Además, la capacidad de los sistemas de IA para aprender y adaptar instantáneamente sus mensajes a sus interlocutores permitirá un nuevo nivel de *microtargeting* y desinformación personalizada.

Los riesgos de manipulación y distorsión de la realidad también crecerán a medida que se generalicen las tecnologías de realidad aumentada y realidad virtual, como *Apple Vision Pro* y *Meta Quest Pro*. Por su parte, las interfaces cerebro-ordenador, como *Neuralink* de Elon Musk, podrían dar acceso sin precedentes a nuestros datos neuronales, ofreciendo información sobre cómo nos sentimos o pensamos a cualquier actor malintencionado. Esto les permitiría piratear y alterar nuestra percepción de la realidad o incluso influir en nuestro estado de ánimo y comportamiento.

La IA generativa aumentará el volumen de las campañas de desinformación así como su calidad y eficacia

Por más lejano que parezca este escenario, es fundamental prever y comprender los riesgos de los avances tecnológicos en curso a la luz del presente contexto de tensiones geopolíticas. Los ciudadanos deben ser conscientes de cómo se utilizan —y explotan— sus sesgos cognitivos y sus datos en beneficio de terceros, de modo que sean capaces de evaluar críticamente la información que consumen y comparten. Por su parte, a los responsables políticos les corresponde definir y abordar cómo las tecnologías emergentes pueden emplearse en ataques cognitivos, lo cual exige un conocimiento integral de la tecnología, la neurociencia y la geopolítica y supera con creces las medidas de ciberseguridad vigentes. Resulta primordial adaptar los marcos de gobernanza actuales en favor de un equilibrio entre la innovación y los derechos cognitivos individuales. Así como también lo es identificar el tipo de acciones en el ámbito cognitivo que suponen una agresión y cuáles son los mejores mecanismos de atribución y rendición de cuentas.

En todo caso, las autoridades no deben limitarse a evaluar en qué medida las nuevas tecnologías facilitan la guerra cognitiva y cómo pueden regularse para evitar usos fraudulentos, sino que también deben colaborar con una amplia diversidad de actores, desde psicólogos hasta ingenieros, a fin de identificar las vulnerabilidades de la cognición humana y cómo utilizar la tecnología para entenderlas y abordarlas.

Lo que parece claro es que no hay tiempo que perder. Las capacidades para llevar a cabo la guerra cognitiva no dejarán de aumentar, y con ello cambiará tanto el carácter de los conflictos como la forma de afrontarlos. Si actuamos pronto podremos crear un panorama tecnológico que suponga un beneficio, y no una carga —o algo peor—, para la autonomía del ser humano y la sociedad en general.