Vencer convenciendo o, si es preciso, combatiendo

ILUSTRACIÓN: JEFF BENEFIT

Lo que diferencia a las operaciones militares basadas en afectos de las acciones tradicionales no son los objetivos sino la utilización psicológica y propagandística para las que están diseñadas. Se trata de la utilización de las redes sociales para manipular las emociones y los afectos con el objetivo influenciar a audiencias propias o del adversario

El diccionario Oxford eligió posverdad como la palabra del año 2016 en el mismo momento en que se estaba empezando a asimilar el alcance de las filtraciones de correos electrónicos y otras informaciones durante la campaña electoral estadounidense[1]

La posverdad hace referencia a "circunstancias en las que hechos objetivos influyen menos en la formación de la opinión pública que lo que lo hacen los llamamientos a emociones y creencias personales"[2]. Se trata de circunstancias en las que la verdad no se puede contrastar fácilmente o, al menos, inmediatamente; en las que los hechos nos resultan remotos o confusos. Son oportunidades para que "una mentira repetida adecuadamente mil veces, se convierta en una verdad", en palabras de Joseph Goebbels, el ministro nazi de propaganda de Adolfo Hitler.

No se trata, por lo tanto, de un fenómeno nuevo[3]. No obstante, el auge de los populismos y algunos sorprendentes resultados en elecciones y referendos lo han traído a la primera línea de la actualidad mediática y política. Algunos indicios parecen señalar que individuos u organizaciones ubicados en la Federación Rusa puede estar detrás de las campañas para posicionar a varios de estos líderes y partidos[4]. La sociedad y la clase política han mostrado su interés y preocupación por la utilización de ataques informáticos como base de partida para la manipulación de los sentimientos de los votantes.

De hecho, la Unión Europea ha creado ya un centro especialmente dedicado a combatir este fenómeno, la *East Stratcom Task Force* o Agrupación de la Comunicación Estratégica del Este. Estas prácticas también han interesado vivamente a las comunidades de defensa e inteligencia. La OTAN tiene también un *think-tank* asociado relacionado con el mismo asunto, el Centro de Excelencia de Comunicación Estratégica de la OTAN, en Riga, Letonia[5]. Las últimas estrategias nacionales de seguridad en España y en Estados Unidos también recogen esta amenaza entre sus nuevas prioridades.

Lejos de requerir de sofisticadas herramientas cibernéticas, **estos ataques son relativamente simples de realizar desde el punto de vista informático**. Una preparación basada en la correlación de datos mediante *big data,* un ataque de *phishing* para acceder a las claves de algún usuario y una difusión de los resultados en bases de datos almacenadas en la internet profunda o *deep web* y distribuidas en portales como *Wikileaks*.

La distribución, cuidadosamente dosificada, de la información obtenida a través de foros y redes sociales se amplifica después mediante grupos –de humanos y de robots– que inundan el espacio informativo y despiertan la curiosidad. Desde ahí, es capturada por la prensa –muchas veces de forma acrítica– que le presta de este modo su sello de credibilidad. Se consuma así el paso de la infección desde las redes digitales a

las neuronales y sociales, en las que realmente desarrolla su efecto.

¿Puede alguien dudar a estas alturas que la solvencia del sistema democrático o, simplemente del sistema electoral, es un recurso crítico para los países de Occidente? ¿Cabe alguna duda sobre una criticidad similar en el caso del sistema bancario? Por lo tanto, si la Estrategia de Seguridad Nacional recoge la protección de las infraestructuras críticas y los servicios esenciales como una de las prioridades para España, ¿no parece lógico pensar que la protección de los mismos debe extenderse a estos conceptos, no tan tangibles como las comunicaciones o la energía, pero no menos consustanciales con el mantenimiento de nuestros valores y nuestro modo de vida?

> En una época de engaño universal, decir la verdad es un acto revolucionario". George Orwell

Qué porcentaje de verdad haya en el mensaje es poco importante. En el mundo de la posverdad, la realidad es irrelevante[6], lo verdaderamente importante son las percepciones que se tienen. En este sentido, hay tres factores clave que llegan de la mano de las tecnologías de la comunicación digitales: la democratización y desprofesionalización de la generación de contenidos informativos, la interactividad del medio y la saturación de información disponible, o infoxicación.

En cuanto a la democratización de la generación de contenidos, la ruptura del monopolio estatal del uso de la fuerza ha venido acompañada de una pérdida similar de privilegios en lo que se refiere a la comunicación. La democratización de las comunicaciones, primero con la apertura de múltiples canales de radio y televisión a empresas privadas con intereses propios y diferenciados de los estados, y después con la llegada de internet y las redes sociales, ha cambiado radicalmente esta ecuación.

En el moderno mundo de la comunicación se producen fenómenos paradójicos y, muchas veces, contradictorios. La multitud de fuentes, la inmediatez del acceso a los contenidos y las propias posibilidades que ofrece la tecnología para distorsionar los hechos provocan que un mundo que debería ofrecer una mayor facilidad para discernir lo verdadero de lo falso, se encuentre a merced de aquellos que controlan las técnicas adecuadas para la generación y difusión de los contenidos.

Contenidos virales

A pesar de los numerosos estudios que exploran los mecanismos por los cuáles un contenido se transforma en viral, no es siempre posible explicar qué hace que uno alcance una difusión millonaria y otros pasen desapercibidos. Sin embargo, la propia naturaleza humana y las dinámicas de grupo favorecen un mayor crecimiento de aquellos contenidos que, bien coincidan con nuestras propias convicciones previas, bien justifiquen o apoyen alguna creencia o práctica propia. La explotación de esta difusión por parte de actores, estatales o no, otorga un enorme poder al generador del contenido.

El documento del Atlantic Council titulado "*Dynamic Stability: US Strategy for a World in transition*"[7] condensa muchas de estas ideas en apenas unas líneas. Afirma que en el mundo *postwesphaliano* las percepciones se convierten en realidades a base de que más información llegue a más gente a través de más canales que nunca en la historia. Para acometer la tarea de configurar estas percepciones, concurre con Kristin Lord en la

necesidad de ir más allá de la diplomacia pública en las estrategias de acometimiento de las audiencias objetivo.

Las percepciones se convierten en realidades porque más información llega a más gente a través de más canales

Incide el mismo documento unas líneas más adelante en el factor diferencial de la interactividad del medio digital respecto de las comunicaciones tradicionales a través de la prensa, radio o televisión. El poder de las redes sociales digitales nace de la combinación de su alcance, su inmediatez y su interactividad y es tan comparable con los otros medios como lo es una bomba tradicional con una bomba atómica. Son cualitativamente diferentes. De hecho, tanto en su explotación[7], como en su protección[8]sus gestores están mostrándose muy activos. También lo están siendo sus usuarios, con la aplicación de inteligencia artificial a la creación de perfiles automatizados[9] o con la profesionalización de la figura del c*ommunity manager* en la gestión de procesos políticos[10]. Los *influencers*[11]se han convertido en las estrellas mediáticas digitales.

La interactividad introduce al elemento humano en la comunicación, lo involucra en la misma, y apela a su empatía para captar y retener su atención. **El mensaje bidireccional cala mucho más profundamente en el sujeto** en tanto que este deja de ser pasivo y pasa a formar parte de la cadena de la comunicación. El sentimiento de pertenencia y de comunidad acentúa todavía más la interiorización de los mensajes. La necesidad de aceptación por parte de los sujetos, la voluntad de destacar, la satisfacción del ego y otros factores potencian el mensaje y, sobre todo, sus "efectos afectivos".

Finalmente, la infoxicación o saturación de contenidos. El ciudadano medio del siglo XXI tiene una muy limitada capacidad para asimilar razonamientos complejos. De hecho, un estudio psicológico revela que el tiempo que tiene un candidato electoral, por ejemplo, para hacer llegar su mensaje al electorado manteniendo su atención se ha reducido en las últimas décadas desde los cincuenta segundos a los poco más de ocho actuales[12].

Conviene tener presente que el centro de gravedad de todos los conflictos es el ser humano. Da igual lo tecnificado que sea un entorno. Al menos por el momento, las decisiones últimas las toman las personas, aunque luego puedan ejecutarlas las máquinas en algunos casos. Es la persona la que se constituye como el objetivo de nuestras acciones de influencia, de nuestros mensajes.

Consolidación de las narrativas

La infoxicación es un componente esencial en la consolidación de las narrativas y de las *fake news*. El "*zapping* informativo" a que nos someten las redes sociales y los medios de comunicación contemporáneos –con un aluvión de ideas y conceptos que apenas da tiempo a asimilar y, mucho menos, a verificar– obliga al receptor a digerir apresuradamente las percepciones. A partir de ahí, debe conformar su idea del mundo en

base a narrativas que, muchas veces, tienen como única base científica la repetición de estas ideas por millones de voces, humanas o no, tan poco informadas como él mismo.

La inasumible cantidad de datos a los que el empresario, el comandante militar, o el ama de casa tienen acceso en la actualidad genera una intoxicación de información que hay que gestionar en varios sentidos. En primer lugar, diferenciando los hechos de las opiniones, la realidad de la interpretación. Después, siendo capaces de correlacionar los distintos datos y enfoques para obtener una visión de conjunto que ofrezca la solución más eficiente al problema. Finalmente, estableciendo límites a la cantidad de información que se va a requerir antes de adoptar una decisión para evitar demorar la misma con diferenciales despreciables de detalle.

Aunque estas fases se corresponden perfectamente con el ciclo de decisión propuesto por el coronel de la Fuerza Aérea de Estados Unidos John Boyd (ciclo OODA –Observación, Orientación o estudio, Decisión y Acción–), la observación en la era digital produce tantos resultados que se dificulta la orientación y se demora la decisión en espera de nuevos datos. Se ha pasado de un ciclo en el que la observación y el análisis consumían la mayor parte del tiempo y las energías a uno en el que ambos factores se producen de forma automática en base a motores de búsqueda y técnicas de *big data*.

Se trata de la utilizar las redes para manipular los afectos y las emociones

Las Fuerzas Armadas tienen que estar preparadas para combatir y vencer. El aforismo, repetido por militares de todas las generaciones, es innegable. Pero eso no significa que el combate tenga que ser la primera ni la más deseable de las actuaciones de los ejércitos. El objetivo es vencer la guerra, no ganar el combate. Mejor, pues, decir que las Fuerzas Armadas tienen que estar preparadas para vencer, combatiendo, si es preciso; convenciendo, si es viable.

Decía Sun-Tzu que “un verdadero maestro de las artes marciales vence a otras fuerzas enemigas sin batalla, conquista otras ciudades sin asediarlas y destruye a otros ejércitos sin emplear mucho tiempo”. Sus palabras están más vigentes que nunca, ya que el maestro del engaño –como se le ha llamado– se habría encontrado en su elemento en este siglo XXI.

En el argot militar, las Operaciones Basadas en Efectos (EBAO) son aquellas que buscan conseguir efectos políticos o estratégicos mediante misiones tácticas convencionales[13]. La destrucción de una central eléctrica busca la paralización de la industria de defensa de una región concreta, por ejemplo. El objetivo son las capacidades, no las infraestructuras.

El campo de batalla de la comunicación

Las operaciones basadas en afectos englobarían mucho más que los ataques de carácter estratégico-político y que se atribuyen, respectivamente, a un actor estatal –como la Federación Rusa– y a uno que mantuvo pretensiones de estatalidad –como el Dáesh, el autodenominado Estado Islámico. No es este el lugar ni el momento de valorar la autoría última de los ataques, pero sí de tomar en consideración lo difusa que es en la actualidad la separación entre los distintos tipos de actores y la progresiva pérdida del monopolio en el uso de la fuerza de los Estados característico del mundo *wesphaliano*.

Estas operaciones se desarrollan a todos los niveles, desde el estratégico al táctico. De alguna forma, muestran cómo se ha ampliado el campo de batalla tradicional o, mejor dicho, cómo se ha extendido el campo de actuación de las Fuerzas Armadas al conjunto de la acción del estado con la inclusión de líneas de acción que no se contemplaban hasta hace muy poco tiempo. Difícilmente puede argumentarse que una amenaza para la seguridad nacional como esta no caiga, siquiera parcialmente, dentro del ámbito de actuación militar.

Las operaciones basadas en afectos no tienen por qué variar en su forma respecto de las que se venían realizando hasta ahora. De hecho, a nivel táctico, **se podrán atacar objetivos idénticos a los que se incluirían en una campaña puramente cinética**, aunque su significación y los efectos afectivos serán muy distintos, bien por su oportunidad temporal o por la utilización mediática que se haga de los mismos. La destrucción de la misma central eléctrica –o su neutralización mediante un ciberataque, como en el caso de Ucrania– busca la pérdida de confianza de la población respecto de los servicios proporcionados por las empresas ucranianas y su captación por proveedores rusos. El objetivo, esta vez, son las personas.

Lo que diferencia a las operaciones basadas en afectos de las acciones cinéticas tradicionales no son los objetivos, sino la utilización psicológica y propagandística que se hace de las mismas. Cuando el Dáesh asesina –que no ejecuta– a sus prisioneros de un tiro en la nuca, con disparos de un cañón de artillería antiaérea, degollándolos en una playa o asándolos vivos, el resultado sobre el terreno es el mismo. Sin embargo, su difusión a través de las redes sociales y las publicaciones digitales de la organización terrorista convierten estos actos en símbolos –de poder para sus partidarios, de terror para sus adversarios– y en un arma en sí misma.

Del mismo modo, no es la intrusión en las cuentas de correo electrónico del Consejo Nacional Demócrata lo que provoca efectos en las elecciones estadounidenses, sino la publicación de lo obtenido a través de Wikileaks en dosis medidas y administradas con una posología muy concreta, eligiendo aquellos momentos en que su repercusión alcanzaría su máximo alrededor de la jornada electoral.

Secretos inconfesables

No se trata de revelar secretos inconfesables, ni siquiera verdades probadas, sino de provocar sentimientos de indignación o de repulsa que lleven al rechazo de una idea o de una persona. El objetivo es el corazón más que el cerebro, los sentimientos más que la razón[14].

Su reiteración termina, además, por elevar el umbral de violencia ante el cual reacciona la opinión pública. La exposición continuada a actos de barbarie empieza generando una conciencia del problema para terminar por habituar al público a su presencia constante y conseguir que se asuma como una realidad, triste pero inevitable. La creación de bots que reiteran los mensajes o los apoyan en diferentes medios responde a la necesidad de herramientas que hagan uso de las facilidades que ofrece el ciberespacio para desarrollar esta técnica.

Será preciso, por lo tanto, acomodar medios, doctrinas, técnicas, tácticas y procedimientos a una guerra 3.0[15]en la que el espectro electromagnético no es simplemente un medio a través del cual transmitir instrucciones, sino que se convierte en un escenario más de la batalla y, al mismo tiempo, en una poderosa arma, si se coloca en las manos adecuadas (Greenberger, 2017). **La comprensión de esta nueva realidad es urgente** y requiere una adaptación continua a un cambio exponencialmente acelerado (Der Derian, 2017).

Moscú ha entendido mejor que nadie la interacción entre la psicología y la sociología, y la cibernética. Sheera Frenkel afirma[16], de hecho, que Rusia está escribiendo el nuevo manual de la guerra cibernética, en referencia a su inclusión dentro del concepto de la guerra de la información y a su utilización para el posicionamiento de la Federación Rusa en la escena mundial[17]. No es casual que Valeri Vasilievich Gerasimov, autor ya en 2013 de

publicaciones que anunciaban la estrategia que lleva su nombre[18] y que priorizan el fortalecimiento de estos conceptos, sea el actual Jefe de Estado Mayor de las Fuerzas Armadas rusas.

La guerra en los corazones y las mentes[19]

Dice el papa Francisco que, más que una era de cambio, estamos viviendo un cambio de era. Las implicaciones de la digitalización de nuestro mundo y de la aceleración exponencial de los cambios que tienen lugar en él van mucho más allá de lo cotidiano de nuestras vidas domésticas. Desgraciadamente, el ciberespacio no elimina solo las fronteras horizontales entre los estados, sino también las verticales entre estos mismos estados, las corporaciones y los individuos. La guerra es una manifestación más de la política y de la sociedad, y en sus formas más modernas, vuelve a estar entre la gente a través del ciberespacio.

Se trata, en definitiva, de la utilización de las redes para manipular los afectos y las emociones como forma de influenciar lo que siempre ha sido y será el centro de gravedad de todas las operaciones: el ser humano.

Greenberger, M. (2017): What Happens When Personal Information Gets Weaponized", Berggruen Institute. Disponible en http://philosophyandculture.berggruen.org/ideas/what-happens-when-personal-information-gets-weaponized

Der Derian, J. (2017): The Cyber Age Demands a New Understanding of War But We'd Better Hurry. Berggruen Institute. Disponible en http://philosophyandculture.berggruen.org/ideas/the-cyber-age-demands-a-new-understanding-of-war-but-we-d-better-hurry

Pavel, B.; Engelke, P. y Ward, A. (2015): Dynamic Stability: US Strategy for a World in transition. Atlantic Council. ISBN: 978-1-61977-992-1. Disponible en: https://es.slideshare.net/atlanticcouncil/dynamic-stability