Ángel Gómez de Ágreda

Es coronel del Ejército del Aire, Diplomado de Estado Mayor, de Seguridad de Vuelo y de Logística Militar. Máster en Terrorismo por la Universidad Internacional de La Rioja y doctorando por la Universidad Politécnica de Madrid en Ingeniería Industrial.

Piloto de transporte y paracaidista. Fue miembro y jefe de la Patrulla Acrobática de Paracaidismo del Ejército del Aire (PAPEA) y del Equipo Nacional de Paracaidismo. Ha sido profesor en el Departamento de Estrategia y Relaciones Internacionales del Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Jefe de Cooperación del Mando Conjunto de Ciberdefensa y analista geopolítico en la Secretaría General de Política de Defensa, puesto que ocupa actualmente. Ha participado en cuatro misiones internacionales, dos en la Antigua Yugoslavia, una en Afganistán y una en África.

Es autor del libro *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*.

Coronel del Ejército del Aire

Twitter: @AngelGdeAgreda

I-ntentando e-xplicar LO QUE SIGNIFICA LA CIBERSEGURIDAD

Ángel Gómez de Ágreda

Hace unos años corría por las redes una versión "actualizada" de la pirámide Maslow, la que se toma como referencia para determinar la jerarquía de las necesidades humanas. En la base de la versión original de 1943 aparecían las necesidades fisiológicas como el escalón inferior, más urgente y necesario para las personas. En la adaptación digital, el acceso a Internet se colocaba por debajo de la exigencia de comida, bebida y cobijo, y de la seguridad. Al fin y al cabo, cualquier internauta puede pasarse horas sin comer o beber, pero muchos sufrirían terriblemente con una abstinencia similar de acceso a las redes.

Incluso si seguimos con la parodia que, medio en broma, medio en serio, apareció en numerosos memes, la tozuda realidad nos demuestra que por debajo de ese escalón de acceso digital tenemos que colocar otro que garantice una cierta seguridad de ese acceso. Vivimos en un mundo físico con necesidades fisiológicas y, cada vez más, en uno lógico en el que tenemos necesidades digitales. Sin embargo, como seres humanos, seguimos teniendo en ambos la urgencia de sentir que jugamos en un entorno en el que existen reglas y límites.

Eso no significa que esas reglas y esos límites sean los mismos en ambos entornos. Adelantemos ya desde el principio que no lo son. Y también que confundir las normas y los ritmos de los dos es un error tan grave como frecuente entre los "inmigrantes digitales", aquellos que todavía aprendimos a escribir con lápiz antes que con un teclado. En un mundo estamos hechos de carne y hueso, en el otro de unos y ceros, de datos que conforman lo que serían nuestras actitudes y nuestras aptitudes, nuestras filias y nuestras fobias, nuestras virtudes y nuestros vicios, y que exponemos a miles de millones de personas y cosas que las observan desde el otro lado de la pantalla o el teclado, incluso cuando no estamos siendo conscientes de revelar ningún dato.

Nuestra vida tiene lugar en ambos mundos simultáneamente. Eso supone que estamos antropológica y psicológicamente situados entre lo físico y lo digital. Por lo tanto, nuestros avatares —los nombres que nos representan en el ciberespacio, en nuestro correo electrónico, nuestras redes sociales, etc.— se relacionan entre ellos virtualmente siguiendo patrones sociológicos y políticos. Dentro de los primeros están las amistades y los amores, las relaciones comerciales y grupales que surgen en Internet, pero también los crímenes y la delincuencia cibernéticas. Y entre los políticos tendremos una capacidad de debatir y negociar, de formar alianzas y construir proyectos sin precedentes hasta el momento. Pero también tendremos la que, pese a que nos cueste admitirlo, es la forma última de hacer política: los conflictos y la guerra.

Nos hemos acostumbrado tanto a dejar nuestra seguridad en manos del Estado o de terceros que nos cuesta asumir que tengamos que contribuir activamente a ella

No conviene dramatizar en exceso ni alimentar expectativas exageradas. Internet no es más que un nuevo entorno en el que desarrollar la actividad humana. Un entorno, si se quiere, que potencia todo aquello que hay de bueno y malo en nosotros, que nos permite llevarlo mucho más lejos, a más gente y más rápido. Un entorno incluso más humano que los naturales, ya que lo hemos diseñado nosotros. Es nuestro comportamiento, tanto individual como colectivo, el que determina lo que ocurre en los dos mundos. Nuestra responsabilidad es que siga siendo así.

1 Ciberseguridad

Escribir sobre los riesgos y amenazas de la ciberseguridad a estas alturas conlleva el riesgo de repetir lugares comunes con que nos bombardean la prensa y las redes sociales todos los días. Todo el mundo tiene la idea difusa de que hay virus en el ambiente digital, de que nos intoxican con fake news y de que Alexa nos espía. Y a casi todos parece darles igual. Total, ¿quién va a querer espiarme a mí? ¿No me viene incluso bien que me manden anuncios de ofertas de viajes cuando estoy a punto de irme de vacaciones?

Otra cosa es que tengamos claras las consecuencias de esa falta de seguridad en el ciberespacio. Cuando el anuncio de las vacaciones nos llega con un precio creciente cuanto más interés ponemos en encontrar viajes, cuando los productos que nos ofrecen dependen del lugar desde el que nos conectemos, de nuestro nivel de vida, nuestros hábitos o nuestras creencias y cuando eso supone que una parte del mundo resulta invisible a nuestros ojos porque nunca llega a nuestro móvil o a nuestro portátil, entonces empezamos a ver dónde está el problema.

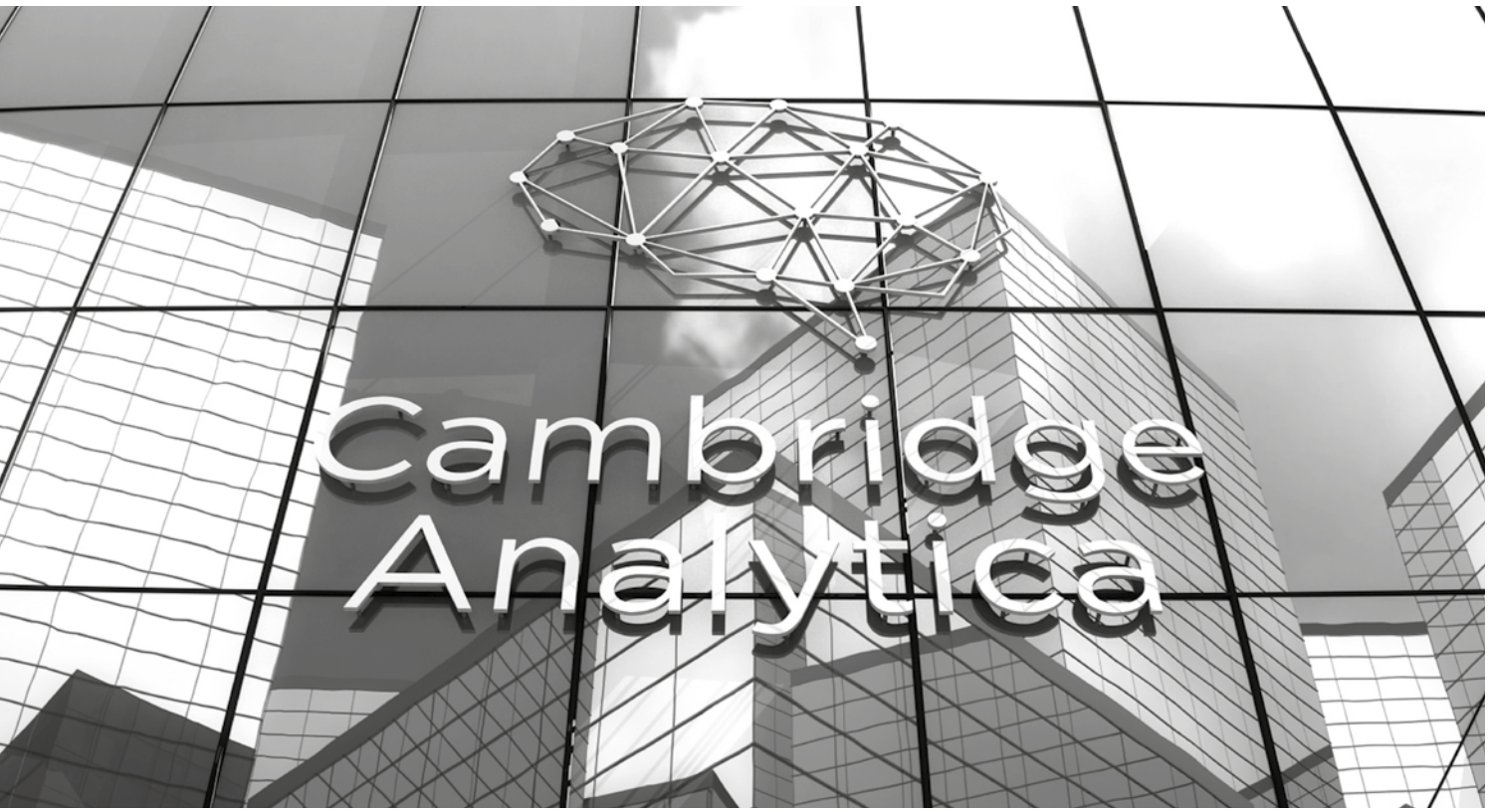
Pero, para entonces, normalmente ya hemos caído en la trampa de la comodidad. En el viejo dilema entre seguridad y libertad, en el contrato social de Rousseau, hemos dejado que ambos platos de la balanza acaben abajo. Hemos perdido nuestra libertad para elegir porque nos hemos convertido en seres transparentes para aquellos que tienen nuestros datos y que nos entregan la información que consumimos. Privados de la verdad, no solo por la mentira, sino por la ocultación de una parte de la realidad, hemos dejado de tener la capacidad para elegir. Y hemos perdido nuestra seguridad porque era el paso necesario para convertirnos en transparentes.

Hemos dejado nuestra libertad y nuestra seguridad en el mismo cajón en el que hemos depositado nuestros datos. Hemos renunciado a las dos a cambio de la comodidad del acceso inmediato y, aparentemente, gratuito a servicios que no habíamos sentido necesidad de tener hasta ahora o que, incluso, no existían hasta hace unos meses. Estamos camino de convertirnos en seres teledirigidos por empresas o por instituciones que saben todo de nosotros y, por lo tanto, pueden manipularnos impunemente.

Ejemplos de cómo la comodidad, la curiosidad, la conveniencia o la inmediatez nos hacen relajar nuestras defensas se encuentran fácilmente en el día a día. El "reto de los diez años" en que se nos invitaba a subir una foto actual y otra de hace una década, o la aplicación FaceApp, que nos "envejece" siguiendo patrones —bastante simplistas, por cierto— de inteligencia artificial, son solo dos de los múltiples cebos que nos ofrecen para que contribuyamos con nuestros datos a aplicaciones que, después, obtendrán millones de la agregación de los mismos.

No parece que ejemplos como el de *Cambridge Analytica* hayan hecho mucha mella en la mayor parte de la población. Igual que ataques de *ransomware* como el famoso Wannacry tampoco consiguieron concienciar a las empresas de la necesidad de mantener el software de sus equipos actualizado. Nos hemos acostumbrado tanto a dejar nuestra seguridad en manos del Estado o de terceros que nos cuesta asumir que tengamos que contribuir activamente a ella.

Y, sin embargo, la seguridad no es gratuita, ni nunca completa. Ni siquiera es algo que puedas medir como tal. Es más un sentimiento que una realidad tangible. Y es muy fácil sentirse seguro detrás del cristal de una pantalla mientras miramos a la parte del mundo que algunos quieren enseñarnos desde el conocimiento de nosotros que les da estar viendo cada una de nuestras acciones. La libertad tampoco es gratuita (*Freedom is not*



Free reza la frase que se refleja en la fuente del Memorial a los Veteranos de la Guerra de Corea, en Washington). La libertad se construye sobre la verdad y el conocimiento. El hecho de que el conocimiento nos llegue cada vez más a través de Internet hace que la defensa de este sea un elemento crítico en la de la libertad.

Conocer el ciberespacio se convierte en algo tan vital — si no más— como conocer el barrio en el que vivimos, nuestro ambiente de trabajo, las normas sociales y las convenciones por las que nos guiamos, y las reglas jurídicas que definen nuestro comportamiento en el mundo físico. La diferencia fundamental es que una buena parte de ese mundo se rige por leyes naturales inmutables, mientras que el ciberespacio es una construcción humana que evoluciona a un ritmo exponencial, y cuyas leyes, términos y condiciones de uso pueden ser y son revisados constantemente.

Cabe pensar que hemos diseñado un mundo solo aparentemente amigable, basado en una estructura reticular cuya fortaleza está en las relaciones y no en los individuos, que privilegia por lo tanto a los grupos más numerosos, a las corporaciones y los Estados sobre las personas. Un mundo cuya evolución somos incapaces de seguir. Que se basó en su diseño en criterios de usabilidad sin plantearse nunca la seguridad al estar pensado para una comunidad cerrada que se convirtió en universal. Un ciberespacio que creció básicamente desregulado para seguir favoreciendo ese crecimiento desenfrenado, aposentado sobre la idea de un usuario altruista, colaborativo e ilustrado.

Y es cierto que, durante su etapa "hippie", Internet creció pensando que la Declaración de Independencia del Ciberespacio de John Perry Barlow era posible. Creyendo en un mundo en el que la información iba a fluir libre y universalmente para provecho de todos y de cada uno, en el que el ciudadano podría participar directamente en la toma de decisiones aprovechando las conexiones para revivir la democracia ateniense clásica.

Internet proporciona todo este potencial y bastante más. Jamás se habría podido secuenciar el genoma humano o desarrollar la economía del siglo XXI sin esa capacidad para relacionar datos de miles de millones de cosas y personas. Pero la información no fluye siempre libremente, sino que lo hace dirigida y digerida, la participación ciudadana se ve condicionada por esa falta de acceso a la realidad y, a falta de esta verdad, hemos recurrido a la reputación efímera de las redes como criterio para construir nuestras certezas.

Desde luego, tenemos que construir una red segura. Necesitamos diseñar sistemas robustos que garanticen la confidencialidad, integridad y disponibilidad de nuestros datos. Debemos proveernos de soluciones técnicas que hagan muy difícil el acceso a nuestros sistemas, de soluciones sociales que supongan normas de comportamiento cívico en Internet y de soluciones legales que blinden los huecos que se puedan explotar técnica o socialmente. Pero, para todo ello, primero necesitamos comprender qué supone la llegada del ciberespacio y cómo ha cambiado nuestras vidas y nuestros valores.

En un rápido repaso de las principales características distintivas del ciberespacio, más allá de su naturaleza artificial, podríamos empezar por su alcance universal. Las audiencias a las que nos dirigimos a través de las redes no tienen limitación para lo bueno o para lo malo. Es casi imposible para un usuario normal segmentar su relato en función de la audiencia, igual que es complejo acotar la información que se recibe. Esta tremenda exposición obliga a considerar la transparencia como una necesidad básica. Todo lo que está en la nube es susceptible de ser visto por alguien y, con tanta gente y tantos sistemas inteligentes buscando, lo será. Solo desde la construcción de un relato coherente se pueden defender posturas en el futuro sin tener que adoptar maniobras defensivas poco creíbles.

No se trata solo de aquellos datos que transmitimos conscientemente. Como afirma Marta Peirano, el sistema conoce todo sobre cada uno de nosotros. Nuestra forma de teclear, de mover el ratón, de andar cuando llevamos el móvil encima (que es siempre), los horarios a los que realizamos cualquier actividad, los lugares por los que nos movemos, todo forma parte de una gran base de datos que el Gran Hermano va construyendo y de la que va extrayendo un perfil sobre nosotros, como individuos y como grupo, mucho más preciso del que tenemos nosotros mismos.

El gran salto vino de la mano de la movilidad. La cantidad de datos que percibe, acumula y transmite cualquier *smartphone* supone un filón de conocimiento para las compañías que están detrás de su fabricación o funcionamiento. Y, muchas veces, de los Estados que tienen jurisdicción sobre las infraestructuras de dichas empresas. No hay movimiento, por leve que sea, que escape a la sensibilidad de los giróscopos de nuestros móviles. Su función principal no es que hablemos por teléfono —de hecho, cada vez los utilizamos menos para eso— como demuestra el hecho de que se reserven siempre una carga remanente de batería después de dejar de servirnos a nosotros para seguir estando en condiciones de enviar los datos que realmente les dan sentido.

En esas condiciones, ¿no debemos replantearnos el valor de la privacidad en nuestras vidas? No es lo mismo el conocimiento parcial que algunas agencias o empresas tenían sobre nosotros hace unos años que el conocimiento exhaustivo que tienen ahora aquellos que puedan acceder a nuestros datos (y, como ha quedado demostrado, estos están a la venta). Es la misma diferencia que vivir en una gran ciudad o en un pueblo de unas pocas docenas de habitantes. A mayor grado de conocimiento sobre uno, menor grado de libertad para desviarse de la norma tendrá. Cuando se sabe todo sobre ti terminas por ser como un coche de Scalextric, la única opción es circular por el carril.

La interactividad es otra de las características de las redes. Para eso están diseñadas, para que todo el mundo pueda comunicarse y responder. Pero la mente humana acepta mucho mejor las proposiciones en las que participa que aquellas que vienen de terceros. Una decisión consensuada en un "diálogo" se adopta como propia y se incorpora a las convicciones más profundas. Internet es una máquina perfecta de convencer. Por una parte, segmenta el discurso de forma interesada de modo que solo ves una parte de la realidad, por otra te implica en la discusión sobre el asunto del que se trate. El resultado final es que un instrumento diseñado para la transmisión de información de forma horizontal termina por hacerlo verticalmente, de arriba abajo.

La dependencia que los sistemas de mando y control militares actuales tienen de la tecnología hace que una interrupción de los servicios que se prestan a través de las redes digitales tenga el potencial de paralizar a un ejército

Esto último tiene dos matices. En primer lugar, la posibilidad de encontrar personas con pensamientos similares al tuyo con las que jamás hubieras coincidido en la vida física. Eso permite cooperación en investigación, pero también integración de minorías ideológicas o de cualquier tipo que pueden formar su "pandilla" a miles de kilómetros de distancia. Colectivos muy minoritarios encuentran apoyo en las redes, igual que radicalismos que jamás hubieran cuajado por la dispersión de sus miembros terminan por juntar una masa crítica suficiente con elementos dispersos.

El segundo matiz a la distribución vertical de la información —que llevaría a un adoctrinamiento— es la necesidad compulsiva que han introducido los dispositivos (especialmente los móviles) de consumo de noticias. Esta intoxicación de información, *infoxicación*, supone un bombardeo incesante de datos muchas veces no coherentes que no forman un relato. La consecuencia es la falta de elaboración de principios y valores, y la

posibilidad de contrarrestar casi cualquier información con una lluvia de desinformación que conduce a una anarquía y al desinterés general por la realidad.

La universalidad, interactividad, rapidez, movilidad y demás características de la Internet son cualitativamente distintas a lo que había antes de las redes. La seguridad, la privacidad y la libertad se ven afectadas por todas ellas y, por lo tanto, su naturaleza cambia con el cambio del entorno. La ciberseguridad no es otra cosa que la seguridad de siempre, pero entendiendo cuáles son las nuevas amenazas a la misma y las consecuencias de no proporcionarla. Estamos en un equivalente histórico —sinanimus exagerandi, como dirían Les Luthiers— al momento en que los peces abandonaron el medio acuático para vivir en tierra. Las nuevas condiciones llevan aparejada la necesidad de cambiar la forma en que respiramos y la dieta de la que nos alimentamos. Ha cambiado el ecosistema, no la necesidad de seguridad.

2 *Ciberguerra*

La definición de guerra implica un enfrentamiento entre Estados con el fin de imponer la voluntad de uno sobre el otro en el que se alcanza un determinado umbral de violencia. Tradicionalmente, este umbral se medía en un número de muertos o en un grado concreto de destrucción física. Si la guerra es la continuación de la política por otros medios, tendríamos que determinar si los medios cibernéticos pueden considerarse armas y, por lo tanto, dar lugar a un conflicto armado.

Pero este no es el momento ni el lugar para entrar en esos debates. Lo que es relevante es la capacidad de las herramientas cibernéticas para doblegar la voluntad de un adversario. En un mundo que Baumann describe como líquido, en un entorno bélico que empieza a describirse como "zona gris", en una geopolítica en la que los actores pueden o no ser estatales, lo que menos relevancia tiene es el tipo de instrumento que se emplee para obtener la victoria. Se emplean todos y cada uno de los disponibles, desde las sanciones económicas o industriales hasta el terrorismo o la invasión de un territorio por fuerzas mercenarias. El ciberespacio se ha convertido en una más de las formas de actuar en un conflicto.

Pero esta "zona gris" ya no se limita a tiempos en que los embajadores han arrojado sus guantes y declarado formalmente las hostilidades, ni se lucha en los campos de batalla mientras la población espera el resultado del combate desde las murallas de la ciudad. Hoy la guerra se libra EN la gente, dentro de cada uno de nosotros y de nuestros dispositivos, en nuestras cabezas y en nuestros corazones, y en los de nuestros avatares.

La guerra se ha trasladado a los relatos y las narrativas. A través del ciberespacio ha pasado al entorno cognitivo, a nuestro entendimiento y nuestros sentimientos. La guerra ya no es lo que era. O quizás ha pasado a serlo de una forma mucho más intensa. Los coroneles Qiao Liang y Wang Xiangsui lo anunciaban ya en 1999 en su "Guerra sin restricciones". Esa capilaridad que permite Internet, esa capacidad para llegar hasta el fondo de cada uno de nosotros, habilita también a los Estados a traer a guerra a nuestro interior. Y a los no-Estados.

Pero es importante recordar el carácter dual del ciberespacio como entorno y como herramienta también en la guerra. Las grandes potencias se aprestan a luchar en y con él en combinación con el armamento convencional y, si procede, el nuclear. La dependencia que los sistemas de mando y control militares actuales tienen de la tecnología hace que una interrupción de los servicios que se prestan a través de las redes digitales tenga el potencial de paralizar a un ejército.

Esta realidad se comprobó ya cuando Israel fue capaz de bombardear una central nuclear que Siria estaba construyendo en 2007 tras cegar a la defensa aérea siria con un ataque informático. En la actualidad, los planes de ataque incluyen el uso de submarinos especialmente diseñados para atacar los cables de fibra óptica que transitan por el fondo de los océanos, la explosión de artefactos nucleares para generar un pulso electromagnético que "fría" los sistemas de comunicaciones de los satélites, la activación de virus, gusanos y troyanos durmientes en las infraestructuras críticas del enemigo, o la saturación de la capacidad de respuesta de las páginas web.

Se trata de ataques cibernéticos sobre la misma estructura del ciberespacio, pero también sobre infraestructuras de comunicaciones, transporte, banca y finanzas, o servicios públicos. Todo lo que esté conectado o sea conectable, además de nosotros mismos como parte del mundo de la información, es susceptible de ser atacado.

Se cuenta la anécdota de que, preguntado por cómo iba a ser la Tercera Guerra Mundial, Einstein afirmó no saberlo, pero aseguró que la cuarta se pelearía con palos y piedras después de una catástrofe nuclear. El estado actual de la tecnología permite afirmar que esa guerra con palos y piedras empezará a los diez minutos de comenzar la tercera guerra. Y que será después de que hayamos perdido el acceso a todo aparato tecnológico después de la inutilización mutua de las redes informáticas de los contendientes y del resto del mundo.

Vivimos en el ciberespacio tanto como en el mundo físico. Somos anfibios entre dos mundos con reglas distintas. Todo lo bueno y malo que hay en nosotros se manifiesta en los dos, aunque de forma distinta, con herramientas diferentes y con consecuencias desiguales. La seguridad sigue estando en la base de nuestra pirámide y la guerra sigue siendo la cúspide de nuestra forma de enfrentarnos, pero ahora tenemos que entender ambas de un modo nuevo.