"TECNOLOGÍAS DIGITALES Y LOS RIESGOS DE LA CIBERNÉTICA EN LA SEGURIDAD NACIONAL"

Digital Technologies and the Risks of Cybernetics in National Security

Recibido: 06 / 08 / 2019 Aprobado: 31 / 10 / 2019

Coronel
Ángel Gómez de Ágreda
España

El autor es Coronel del Ejército del Aire, Diplomado de Estado Mayor, Máster en Terrorismo y Anti-terrorismo por la Universidad de la Rioja, y Doctorando en Ingeniería en la Universidad Politécnica de Madrid. Ha sido profesor del Departamento de Estrategia y Relaciones Internacionales en el CESEDEN, y jefe de la Sección de Cooperación del Estado Mayor del Mando Conjunto de Ciberdefensa. Actualmente es el jefe del Área de Análisis Geopolítico de la División de Coordinación y Estudios de Seguridad y Defensa de la Secretaría General de Política de Defensa (SEGENPOL). Es piloto militar de transporte, paracaidista y diplomado en Seguridad de Vuelo por el Ejército del Aire, la US Air Force y por la Universidad del Sur de California. Ha participado en cuatro misiones internacionales en la antigua Yugoslavia, Afganistán y el Sahel. Ha publicado un centenar de artículos y participaciones en libros. Es autor de "Mundo Orwell. Manual de supervivencia para un mundo hiperconectado". agomde@ea.mde.es

RESUMEN

Internet, esa herramienta que empleamos a diario para las más diversas actividades, es también un ecosistema en el que convivimos y en el que nos relacionamos. Fruto de esa actividad social y política, la guerra está también presente en el ciberespacio. El mundo digital trae consigo modos más eficientes de gestionar los conflictos y cambia sus características al alterar el escenario en el que tienen lugar. Sin embargo, más allá de las nuevas formas de amenaza que surgen de las redes, la principal alteración que se está produciendo es la desintermediación entre los productos y los consumidores. Esto supone un desafío al modelo de gobernanza en su conjunto y no solo a la estabilidad de gobiernos concretos.

Palabras clave:
Seguridad, libertad, desintermediación, narrativa, desinformación, influencia, afectos, guerra en la gente.

ABSTRACT

Internet, the tool we used daily for the most diverse tasks, is also an ecosystem in which we live and in which we relate to one another. As a result of that social and political activity, warfare is also present in cyberspace. The digital world brings along more efficient ways to manage conflict and changes their characteristics by altering the scenario in which they take place. Nonetheless, beyond these new threats emanating from the networks, the main alteration taking place is the disintermediation between products and consumers. This poses a challenge to the governance model as a whole and not only to the stability of specific governments.

Keywords:
Security, safety, freedom, disintermediation, narrative, disinformation, influence, affection, war within the people.

INTRODUCCIÓN

Lo digital se visualiza desde dos ópticas opuestas. Por un lado, como herramienta cotidiana, aparece como algo ubicuo en nuestras vidas y en nuestro trabajo. Por otro, como tecnología, se percibe como algo sobre lo que no tenemos control directo, algo casi sobrenatural ante cuyo poder no cabe más que plegarse. Por lo tanto, terminamos por asumir como natural llevar un celular en nuestro bolso o nuestro bolsillo sabiendo que, de alguna manera, controla todos nuestros movimientos y palabras.

Porque, hace apenas unos pocos años podíamos todavía argumentar que los riesgos de la cibernética eran asuntos de ciencia ficción o de conspiraciones más o menos increíbles. Ya no es el caso, han salido a la luz suficientes ejemplos de cómo las redes sociales o las tecnologías digitales en general comercian y juegan con nuestros datos como para que no nos quede ninguna duda al respecto.

Sin embargo, pese a saber que nuestra seguridad está en entredicho si no limitamos el acceso de estos aparatos a nuestras vidas, pese a saber que nuestra libertad para elegir está siendo condicionada por el conocimiento casi total que se acumula en las bases de datos sobre cada aspecto de nuestras vidas, pese a todo eso, seguimos aferrados a celulares y servicios digitales como un náufrago a una tabla de salvación.

En el viejo debate entre la libertad y la seguridad, en el contrato social que proponía Rousseau, hemos elegido perder ambas a cambio de la comodidad, la inmediatez y la aparente gratuidad de unos servicios que no sabíamos que requeríamos hasta hace apenas unos meses. Hemos regalado nuestros datos sin ser conscientes de que son nosotros, de que en el mundo digital, son la materia de la que estamos hechos igual que la carne y los huesos nos dan forma en el mundo físico.

Y hemos abrazado estas tecnologías particularmente nocivas desde la consciencia de que son, en muy buena parte, fruto de un estudio sociológico que nos genera una dependencia similar a la de las drogas, el tabaco o el alcohol. Al igual que el paquete de cigarrillos es lo primero que prepara el fumador, nuestro teléfono de bolsillo es lo último que querríamos dejarnos olvidado al salir de casa.

En su novela "1984", George Orwell describía cómo el Estado colocaba una cámara en cada estancia de las casas de los ciudadanos para tener absoluto control sobre sus actividades. En 2019, todos y cada uno de nosotros lleva no ya una, sino dos cámaras de alta resolución permanentemente sobre él y se asegura de que no le falte la batería en ningún momento.

INTERNET, HERRAMIENTA PARA GESTIONAR NUEVAS AMENAZAS

El ciberespacio, ese entorno en el que convivimos compartiendo información a través de equipos informáticos, y la inteligencia artificial se han convertido, como dice Andrew Ng, en la electricidad del siglo XXI. Siguen existiendo "cosas" que no son "smart", que no están conectadas, pero son reliquias de un siglo XX que nos parece a todos ya muy lejano.

Porque la clave es precisamente, que internet, que el ciberespacio, no es solo una herramienta que utilizamos en nuestras vidas. Muy lejos de eso, se trata sobre todo de un entorno en el cual estamos desarrollando nuestra actividad. Vivimos a través de nuestros avatares, en las redes informáticas. Pero nuestros avatares, nuestro correo electrónico, nuestro usuario de cualquier plataforma, no dejan de ser también nosotros. Hemos volcado nuestras vidas en ellos y hemos aprendido a creernos la realidad que se nos presenta a su través.

La realidad, la verdad, se han convertido en una abstracción, en algo imposible de aprehender. Vivimos en un mundo global con implicaciones planetarias. ¿Cómo vamos a poder abarcar todos los múltiples aspectos que presenta?, ¿cómo vamos a estar al día de las últimas evoluciones que se producen, o de las últimas noticias?

Afortunadamente, tenemos una ventana que nos acerca instantáneamente a la realidad de cualquier tema en cualquier parte del mundo. Una ventana abierta de forma instantánea a la situación en tiempo real, a lo más reciente que haya ocurrido. Somos dueños absolutos del tiempo y del espacio con solo teclear tres "w" o señalar con el dedo o con el ratón un enlace en una pantalla.

El problema, sin embargo, es que la realidad que se nos presenta a través de la pantalla está separada de la que existe verdaderamente en muchos grados de magnitud. Es una realidad construida en función de lo que esa misma ventana deja ver de nosotros mismos. Percibimos una realidad hecha a nuestra medida, customizada, tuneada para que sigamos enganchados a ella. Y esa percepción es nuestro mundo hasta el punto de que, si la realidad física desafía el relato que nos llega a través de la pantalla, dudamos antes de nuestros ojos que del criterio de Google.

Esa realidad percibida juega con lo más preciado que nos queda. Regalados nuestros datos, solo nos queda nuestro tiempo y nuestra atención. La economía de la atención busca esclavizar nuestra voluntad a una determinada plataforma o a un medio concreto para que se convierta en referencia y para que su capacidad de influencia sobre nosotros pueda monetizarse por parte de media docena de grandes corporaciones.

Más allá de las "fake news", las mismas noticias que los medios nos hacen llegar cada día tienen una carga ideológica y, sobre todo, sentimental, que se adapta a nuestros prejuicios. Si nos gusta un color, todo se volverá de distintos tonos del mismo.

Grandísima y potentísima herramienta esa que permite a la más marginal de las personas encontrar un alma gemela mucho más allá del limitado alcance de su aldea o de su país. Por muy excéntrica o absurda que sea una idea, seguro que habrá alguien entre 4.000 millones de internautas que la comparta. Sobre todo, porque no tendrá que venir asociada a ningún otro relato. Será una idea aislada. No tendrá que aceptar ni amar a la persona completa, sino solo a una de sus ideas. Para las otras, ya encontraremos a otros candidatos a compartirlas. Ya no existe la marginación porque hemos ampliado el alcance de nuestra comunidad al mundo completo.

Pero tampoco existe la limitación. Ya no tenemos tampoco que negociar con nuestros vecinos, con nuestra pandilla, con el grupo social en el que vivimos ningún aspecto de nuestras vidas. ¿Quién necesita sujetarse a la disciplina de un grupo cuando puede individualizar sus emociones, sus sentimientos y sus creencias? Eso, claro, genera egoísmo, individualismo, radicalización y un sinfín de efectos perversos. Pero, por otro lado, alimenta aquella parte de nosotros que siempre está dispuesta a aceptar una taza más: el ego.

Y volvemos así a las cámaras de los celulares, a las que sirven para hacer fotos de nosotros mismos. Vámonos de viaje a los confines del universo a obtener un primer plano de nuestra cara contra el fondo de tal o cual monumento o atracción. Dejada constancia social de la importancia de nuestro ego, pasemos al siguiente estadio.

Hablábamos de que la ventana nos daba acceso a todo el mundo y también de que lo hacía en tiempo real. Y ahí es donde entra en juego el segundo pecado capital de nuestra vida digital. La adicción a lo último se vuelve obscena. Repasamos una y mil veces los titulares de las noticias recogidas en Twitter sin leer ni una sola de ellas más allá de los 280 caracteres que preceden al enlace.

De hecho, la prensa se convierte en un mero diseñador de titulares que resulten lo suficientemente atractivos para que las redes sociales los recojan y generen tráfico en la página web. El contenido completo de la noticia es más o menos irrelevante porque los "clicks" nacen de los titulares. Al final, es un círculo vicioso en el que nadie lee noticias vacías que no se rellenan porque solo se leen los titulares. Los medios son incapaces de romper la dinámica dando información más allá del encabezado, el público se contenta con una cita de consumo rápido siempre que ésta cambie cada vez que revisa su Tablet o su celular, y el Estado se ve incapacitado para regular este mercadeo con la atención de sus ciudadanos.

Es fácil argumentar que siempre ha habido medios de comunicación que eran capaces de influir en las percepciones del público. Y no faltará razón al hacerlo. En los Estados Unidos de finales del siglo XIX, de hecho, había dos grandes medios dominantes: el de Pulitzer y el de Hearst. Este último, "el ciudadano Kane", demostró su capacidad de manipulación propiciando una guerra contra España que terminó con la presencia española en Cuba.

Sin embargo, por muy sesgado que pudiera ser un medio, por muy limitada que pudiera ser la oferta informativa, existía un discurso. Lo ideal sería que hubiera suficientes medios y que estos fueran independientes de los poderes políticos y económicos. Nuestro problema actual no es la cantidad de medios de hecho, cualquier se convierte hoy en una fuente de "información" y de "noticias" a través de las redes sociales. Nuestro problema es con la independencia y con la calidad de esa información.

Esa misma inmediatez que exigimos, unida a la necesidad constante de novedades, degrada la consistencia de la información que

procesamos. Nada es realmente relevante porque mañana habrá sido sustituido por otro asunto. Además, la sospecha permanente sobre la independencia y solvencia de la información nos hace poner toda ella en cuarentena. De este modo, hemos pasado de tener un par de discursos interesados que generaban un relato coherente para sus lectores a tener una miríada de medios que alimentan una cadena de producción en serie de noticias inconexas que no terminan de encajarse entre ellas para formar un relato. Hemos llegado a un mundo sin narrativas, sin verdades y sin interés porque las haya.

Hasta aquí no hemos hablado siquiera de seguridad nacional, de ejércitos, de defensa, ni siquiera de tecnología como tal. No obstante, hemos llegado a un punto en el que lo que se está cuestionando no es la continuidad de un gobierno, de un dirigente o de una idea, sino la misma esencia del poder tal y cómo lo concebimos, los sistemas de gobierno según los conocemos.

La democracia no se concibe sin capacidad para elegir y la libertad se basa en el acceso a la verdad. A algún tipo de verdad -no nos vamos a poner filosóficos en este punto-. El Estado moderno, desde la Paz de Wesphalia en 1648, se basa en el monopolio que los estados ejercen sobre el uso de la fuerza, sobre su capacidad para proporcionar seguridad -y ejercer coacción- sobre sus habitantes. Todo eso salta por los aires cuando lo hacen las fronteras del ciberespacio y cuando las grandes corporaciones compiten por garantizar privacidad o libertad con los mismos gobiernos.

Todo esto ya ha sucedido antes. Las compañías de Indias holandesa o británica eran tan grandes o mayores que la mayor parte de los países de la época en cuanto a su poder económico e, incluso, militar. Y, a pesar de todo, no dejaban de ser empresas nacionales como lo eran Oil Standard o la Bell Company. Grandes monopolios nacionales sujetos a la regulación del Estado en el que tenían su sede y ejercían su actividad. No es un caso similar a los oligopolios mundiales de la era digital.

Es casi imposible hablar de soberanía en la actualidad sin incluir en el concepto la capacidad para actuar en el mundo de la información y en el ámbito digital. Retener el control de las fronteras físicas se antoja del todo insuficiente cuando los recursos y los activos se mueven en el ciberespacio y en el entorno de lo cognitivo. La acción del Estado tiene que ser capaz de ejercer su autoridad también en esos ámbitos para ser realmente eficaz.

No obstante, una de las características que define al ciberespacio es su naturaleza artificial. Ha sido diseñado, construido y mantenido por el hombre. Concretamente, en su inmensa mayoría, por empresas privadas con ánimo de lucro. Es decir, no podemos hablar, como hacen muchos, de un Global Common en sentido estricto porque toda infraestructura está sujeta, no solo a la jurisdicción de un Estado, sino también a la propiedad de una empresa o particular.

Este carácter artificial supone, por lo tanto, una propiedad sobre las características que tiene la arquitectura y la composición de los sistemas digitales. No existe una terra nullius, un territorio sin dueño sobre el que se pueda ejercer soberanía, sino que estamos empleando medios particulares sobre los cuáles construimos nuestra vida digital. Muchas veces, esta infraestructura convertida en un ecosistema mantiene una agenda propia y genera beneficios en paralelo a los servicios que proporciona.

¿Quién hubiera podido intuir siquiera que una parte casi mayoritaria de la población mundial iba a "habitar" parcialmente en un universo diseñado por una compañía? Y, sin embargo, Google es ese ecosistema en el cual estamos interactuando. Es el equivalente a una estación espacial o a una estación en Marte que hubiera sido diseñada por una empresa y en la cual estableciéramos nuestra residencia. Sujetos todavía a algunas restricciones legales derivadas de la residencia fiscal de la empresa, en todo lo demás estaríamos sujetos a las leyes "físicas" imperantes en la estación según su diseño.

Hemos visto que esas condiciones, los términos de uso de las plataformas, pueden incluir cláusulas tan abusivas como aquella por la que se cedía nuestra "alma inmortal" al prestatario de un servicio al acceder al mismo. El requisito no dejaba de ser una mezcla de broma y de demostración de que nadie presta atención a estos documentos deliberadamente engorrosos, cambiantes y oscuros.

Una segunda consecuencia de la naturaleza artificial del ciberespacio es su intrínseca falibilidad. Como toda creación humana, internet no deja de ser algo imperfecto, pero también es un diseño que siempre tenderá a optimizar el beneficio de su diseñador frente a la seguridad de sus operadores. Internet siempre tuvo como prioridad la usabilidad, incluso cuando John Perry Barlow lanzaba

la Declaración de Independencia del Ciberespacio[1], en el fondo una súplica para que los poderes estatales se mantuvieran al margen de un mundo idealizado en el que todos realizarían aportaciones puramente positivas.

La internet es vulnerable igual como son los vehículos que conducimos o las viviendas en las que habitamos. No por eso dejamos de hacer uso de cualquiera de las tres cosas. La única diferencia entre ellas es de alcance. Mientras que las vulnerabilidades de los vehículos o las casas pueden afectar a un usuario o a un número muy limitado de ellos, internet es el habitáculo y el vehículo de miles de millones de personas -y de cosas- que transitan por ella muchas veces sin la menor consciencia de su fragilidad. ¡Es tan fácil sentirse seguro detrás de una pantalla!

Se puede afirmar que la toma de conciencia de los Estados respecto de esa vulnerabilidad llegó en 2007 con el ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés) que sufrió Estonia. Este pequeño país báltico llevaba siendo independiente poco más de tres lustros. Se había escindido de la Unión Soviética, pero mantenía una importante población rusa entre sus habitantes. A falta de una posibilidad más atractiva, centró su modelo de desarrollo económico en la generación de una industria digital y en el aprovechamiento de las posibilidades que ofrecía un todavía incipiente ciberespacio.

El ataque consistió en la saturación de la capacidad de respuesta de las páginas web del dominio estonio (.ee) durante más de dos semanas. Se lanzaron visitas a los servicios de hospitales, transportes, bancos y demás hasta que sus páginas dejaron de responder. Un país que había fiado todo a lo digital quedó, repentinamente, paralizado. Es fácil imaginar los efectos que una agresión similar -o una mera caída del servicio de internet- podría suponer hoy, doce años después.

El ataque procedía, en último extremo, de Rusia. Parece lógico pensar que se trató de una agresión institucional organizada desde el Kremlin, pero a día de hoy, sigue sin poder probarse. Todo lo que le podríamos achacar a Rusia es que no atendiese a su deber de diligencia debida de desactivar el ataque una vez que se estaba produciendo. Incluso, de haber tomado todas las medidas posibles para evitar que se produjese. Sin embargo, en 2007, pocos países se sentían moralmente autorizados a exigir a otro que tuviese en marcha mecanismos para la lucha contra este tipo de actividades.

España no publicó su primera Estrategia de Ciberseguridad Nacional hasta seis años más tarde, fue de los primeros países en hacerlo. El mundo no era consciente de la dependencia que tenía de la tecnología digital. Hoy, cuando esa dependencia es mucho mayor, esa consciencia apenas se ha incrementado mínimamente.

Estonia aprendió la lección y promovió la creación del Centro de Excelencia para la Cooperación en Ciberseguridad de la OTAN (CCD-CoE)[2], que se situó a pocos metros del lugar al que fue trasladada la estatua del soldado soviético que dio lugar al ataque. También estableció embajadas digitales para situar fuera de su territorio copias de todos los datos críticos de su administración. La idea subyacente era desconcentrar la información para hacer más difícil su acceso a un posible agresor.

La solución, que puede ser viable en el caso de Estonia y sus 1,3 millones de habitantes, supone retos difíciles de abarcar para países más grandes. Y tampoco termina de solucionar el problema de la independencia o la soberanía nacional, sino que lo difiere a aliados con los que, en un momento dado, existe buena sintonía y afinidad.

No asegurar los activos digitales de un país equivale a no hacerlo con las fronteras físicas o con la vida de sus ciudadanos en el mundo físico. No hay alternativa para un Estado funcionante a la asunción de sus responsabilidades en el ciberespacio. Las limitaciones serán muchas en el caso de que no existan desarrollos y plataformas propias, en cuanto no existan redes autóctonas, y siempre que los dispositivos que se utilicen procedan de terceros países, pero no puede dejar de poner todos los medios al alcance de las autoridades nacionales para retener el control sobre los mismos.

Dos son los principales ámbitos en los que se tienen que centrar los esfuerzos de cualquier administración: la protección de sus infraestructuras y servicios críticos, y el aseguramiento de los datos de y generados por sus ciudadanos. Mientras que el primer aspec-

[1]El texto de la declaración puede leerse completo en https://www.eff.org/cyberspace-independence

[2]https://ccdcoe.org/

to debería contribuir a la supervivencia de la nación, el segundo permite la de sus ciudadanos y establece las bases para el desarrollo económico y el bienestar de los mismos. Sin una adecuada defensa del conocimiento como tal no existe posibilidad de progreso social ni económico.

Queda, en fin, hablar de la utilización del ciberespacio en provecho propio. La protección de las redes es un primer paso necesario para poder emplearlas, pero no es suficiente.

Decíamos que internet había nacido y se había desarrollado con la usabilidad como bandera. En nuestro afán por mantener las redes seguras no podemos descuidar la verdadera razón de su existencia. Siendo, como recordábamos más arriba, una creación humana no tendría sentido mantenerla si no proporcionase unas ventajas superiores a los costes de su implantación y mantenimiento.

Es evidente que las tecnologías digitales han cambiado el mundo. Lo han hecho profundamente con los medios de comunicación, están siendo disruptivos en la banca y las finanzas, y podrían -como hemos visto- hacer otro tanto con los Estados y las formas tradicionales de gobernanza. Pero, más allá de esas utilidades en cuanto a la desintermediación entre la noticia y el público, entre el dinero y el cliente, o entre el gobernante y el gobernado, internet nos ofrece posibilidades directas de uso en el mundo de la seguridad y la defensa. Y mucho más sin entramos en el ámbito de la inteligencia artificial que, por ahora, dejaremos en simple mención.

La conectividad, inmediatez y capacidad de procesamiento de información cambian el campo de batalla, concebido desde el punto de vista de las operaciones militares como de las policiales. De hecho, una de las primeras distinciones que elimina el ciberespacio es la que existía entre la seguridad interior y la internacional.

No merece la pena entrar en los detalles de qué significa en la práctica el hecho de que podamos mantener una conexión de datos con cualquier miembro de nuestro equipo esté donde esté en el teatro de operaciones. También parece superfluo deletrear las ventajas que introduce en el planeamiento de las operaciones, en las labores logísticas, en la recopilación y tratamiento de la información y su transformación en inteligencia.

En muchas de estas facetas, internet simplemente proporciona una vía optimizada para llevar a cabo aquello que ya se venía haciendo en el mundo analógico. Un ideal olímpico aplicado a lo físico, podemos hacer lo mismo, pero más alto, más lejos y más fuerte. Sin embargo, siendo importante la contribución que hace en estos campos, no es lo fundamental.

Lo realmente disruptivo, allá donde se encuentra el valor añadido del ciberespacio, son aquellas tareas que configuran un nuevo paradigma de seguridad y de defensa. Igual que digitalizar una empresa no significa hacer en formato MSWord o .pdf lo que antes hacíamos a bolígrafo o con dos copias de calco en la máquina de escribir, tampoco digitalizar el campo de batalla consiste en cambiar el mapa enrollable desplegado en la pared o sobre la mesa por un videowall interactivo. Es el fondo de la guerra lo que cambia, no sólo la forma.

Por eso, lo importante del ciberespacio es que su alcance, interactividad e inmediatez nos permiten -y permiten al adversario- llevar la guerra a la gente. Las grandes explanadas donde se congregaban infantes y jinetes para la batalla dejaron paso a una guerra mucho más cercana. Los terroristas y los guerrilleros trajeron la guerra entre la gente; a nuestras casas, a nuestras calles. El ciberespacio se cuela dentro de nosotros y nos convierte, a cada uno -combatiente o no-, en campo de batalla, en arma y en objetivo al mismo tiempo.

Las redes neuronales del ciberespacio se confunden con las de nuestras mentes para llevar hasta ellas las percepciones de la realidad, para alterar nuestra voluntad apelando a nuestros sentimientos y para vencer -como aconsejaba Sun-Tzu- cada batalla sin llegar a combatir.[3]

Son operaciones que no pretenden destruir físicamente más que en la medida en que esa destrucción envíe un mensaje. No son operaciones basadas en los efectos cinéticos, operativos o logísticos, sino en los afectos y en los sentimientos como precursores de las voluntades.

Esa es la verdadera naturaleza disruptiva del ciberespacio y de las tecnologías digitales, su capacidad para hacer la guerra en la gente. De forma sutil, siguiendo doctrinas antiguas como "la muerte

[3]El libro de Sun-Tzu puede consultarse en https://suntzusaid.com/

por los mil cortes" en la que ninguna agresión es letal ni justifica una respuesta, pero todas debilitan y merman nuestra capacidad de respuesta. Siguiendo doctrinas modernas como la "guerra sin restricciones", en la que todo contribuye al objetivo final, en la que no hay periodos de paz ni de guerra, sino un conflicto permanente de constante cooperación y competición.

CONCLUSIÓN

La consideración del ciberespacio como entorno en el que desarrollamos nuestra actividad trae consigo implicaciones importantes. Al cambiar el escenario, cambia necesariamente la obra representada, nuestra vida entera se ve afectada por las características del medio. Sus características claves son la ubicuidad, la interactividad y la inmediatez, y las tres tienen implicaciones importantes en sus vertientes positiva y negativa.

Si bien la posibilidad de comunicarse con cualquier punto del planeta y con cualquier persona ofrece unas enormes posibilidades que muchas veces no somos conscientes de utilizar a diario, también es cierto que esa falta de limitación respecto de dónde encontrar apoyo a nuestros puntos de vista reduce la autocrítica y la capacidad de crecimiento. Si la interactividad es mucho más poderosa a la hora de comunicar ideas, también lo es cuando se trata de manipular mentes. Si la inmediatez permite una mayor eficiencia en los negocios o en las transacciones, también termina por incrementar la obsolescencia de las noticias hasta convertirlas en carentes de contenido.

La promesa de comodidad y conveniencia que traen consigo los servicios digitales adormecen el afán de lucha y superación tanto del humano como individuo como de la especie como conjunto. Esto genera sociedades de valores poco profundos y nada proclives, por lo tanto a su defensa. Las desigualdades se incrementan y las castas se estratifican, muchas veces en función del acceso dispar a la tecnología y de la comprensión de sus implicaciones.

La guerra, como fenómeno sociológico y político, se vuelve igualmente ubicua e instantánea. Vivimos en un permanente estado de competición, gestionando conflictos en una "zona gris" que se mueve bajo el umbral que generaría una respuesta por parte del adversario. La guerra en este nuevo ámbito se traslada al interior de la gente, a los sentimientos. Son operaciones basadas en afectos en las que no se juega tanto con la realidad como con las percepciones y los relatos. En las que no es necesario alterar lo físico porque se puede presentar distorsionado al público objetivo. Una suerte de realidad aumentada narrada en la que somos capaces de superponer conceptos e interpretaciones sobre una capa de medias verdades.

Es cierto que la seguridad nacional requiere de una defensa de la capa tecnológica, de seguridad de las redes. No obstante, la ciberseguridad, la seguridad del ciberespacio tiene que abordar también a los humanos que viven dentro de él y avanzar hasta la explotación de las posibilidades que se presentan en el mismo como una forma más de preservarnos. En un mundo en el que puedes correr, pero no esconderte, será preciso estar en los puestos de cabeza para siquiera conocer los riesgos antes de que se materialicen.

Todo ello va a suponer la necesidad de formar una y otra vez a un nutrido grupo de profesionales, y de concienciar y formar al resto de la población, que queda subsumida en la guerra como escenario, arma y víctima de la misma.

REFERENCIAS

Allen, T. S., & Moore, A. J. (2018). Victory without casualties: Russia's information operations. *Parameters, 48*(1), 59–71.

Botsman, R. (2015). The changing rules of trust in the digital age. *Harvard Business Review Digital Articles, 2–4.* Recuperado de http://search.ebscohost.com/login.aspx?direct=true%7B&%7Ddb=bth%7B&%7DAN=118685348%7B&%7Dsite=ehost-live

Del-Fresno-García, M. (2019). Desórdenes informativos: Sobreexpuestos e infrainformados en la era de la posverdad. *El Profesional de La Información, 28*(3), 1–11. Recuperado de https://doi.org/10.3145/epi.2019.may.02

Fischer-Lescano, A. (2016). Struggles for a global internet constitution: Protecting global communication structures against surveillance measures. *Global Constitutionalism, 5*(2), 145–172. Recuperado de https://doi.org/10.1017/S204538171600006X

Gómez de Ágreda, Á. (2014). El ciberespacio como escenario del conflicto. Identificación de las amenazas. En Centro de Estudios de la Defensa Nacional. El ciberespacio: Nuevo escenario de confrontación. (pp. 863–868). Madrid, España: Ministerio de Defensa.

Gómez de Ágreda, Á. (2016). De Irak a Irak. Evolución del pensamiento militar contemporáneo. *Tiempo Devorado,* 3, 2–6.

Gómez de Ágreda, Á. (2018a). Falsas noticias, no noticias falsas | Telos Fundación Teléfonica. *TELOS*, 109. Recuperado de https://telos.fundaciontelefonica.com/telos-109-asuntos-de-comunicacion-falsas-noticias-no-noticias-falsas/

Gómez de Ágreda, Á. (2018b). Vencer convenciendo o, si es preciso, combatiendo. *TELOS*, 109. Recuperado de https://telos.fundaciontelefonica.com/una-nueva-doctrina-para-la-guerra-del-siglo-xxi-vencer-convenciendo-o-si-es-preciso-combatiendo/

Gómez de Ágreda, Á. (2019a). La guerra en la gente. *IEEE.*, 14, 1–14.

Gómez de Ágreda, Á. (2019b). *Mundo Orwell: Manual de supervivencia para un mundo hiperconectado* (1st ed.). Barcelona: Ariel.

Gómez de Ágreda, Á., & Robles Carrillo, M. (2016). Tecnología y derecho: El FBI contra Apple. Actas *JNIC*. Recuperado de https://nesg.ugr.es/index.php/en/lineas-6?view=publication&task=-show&id=673

Lewis, J. A. (September, 2018). Cognitive effect and state conflict in cyberspace. *Report*. Recuperado de https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace

Liang, Q., y Xiangsui, W. (Febrary, 1999). Unrestricted Warfare. *PLA Literature and Arts Publishing House,* 1–228. Recuperado de https://www.c4i.org/unrestricted.pdf

Ng, A. (2017). *Artificial intelligence is the new electricity.* Medium. Recuperado de https://medium.com/syncedreview/artificial-intelligence-is-the-new-electricity-andrew-ng-cc132ea6264

Prier, J. (2017). Commanding the Trend : Social Media as Information Warfare. *Strategic Studies Quarterly, 11*(4), 50-85. Recuperado de https://www.jstor.org/stable/26271634?seq=1#metadata_info_tab_contents

Reino de España. (2013). *Estrategia de ciberseguridad nacional.* Recuperado de https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf

Rugge, F. (2018). Mind hacking: Information warfare in the cyber age. *ISPI, 20*(319), 1–8.

Sociología y Redes Sociales. (2010). *La economía de la atención.* Recuperado de http://sociologiayredessociales.com/2010/03/economia-de-la-atencion/

Voiklis, J., Kim, B., Cusimano, C., & Malle, B. F. (2016). Moral judgments of human vs. robot agents. *25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), New York, 2016, 775-780*. doi: 10.1109/ROMAN.2016.7745207