Capítulo segundo

Políticas de seguridad y defensa en la era de la posverdad

Alfonso Merlos

Resumen

La era de la *posverdad* viene marcada por la difusión estratégica a través de campañas metódicas y de alcance global, de informaciones de dudosa veracidad y de historias falsas que, en determinados procesos políticos y electorales, pueden representar una amenaza para la seguridad de los Estados y de la propia comunidad internacional. Las guerras de información basadas en el uso masivo y estudiado de las nuevas tecnologías de la comunicación exigen de nuevas estrategias de defensa que identifiquen con precisión la fisonomía de estos nuevos riesgos y sean capaces de atacarlos, neutralizarlos y amortiguarlos en sus efectos. Los planes y mecanismos a desarrollar e implementar tendrán forzosamente un carácter, en el corto plazo, dinámico y transformacional.

Palabras clave

Política, seguridad, defensa, *posverdad*, comunicación, inteligencia, redes sociales.

Abstract

The era of "post-truth?" is characterized by strategic diffusion, through methodic and global reach campaigns, untruthful information, and false stories that specific politic and electoral processes can represent a threat for the security of the states and for the international community. The information battles based on the massive use and studies of the new communication technologies require new defense strategies that identify precisely the physiognomy of these new risks and its ability to attack them, neutralize them, and reduce its effects. The plans and mechanisms to be developed and implemented will have to forcefully have a character, in the short run, dynamic and transformational.

Keywords

Politics, security, defense, "post-truth", communication/s, Intelligence, networks, social.

Introducción: un futuro de incertidumbre y fragilidad

En la actual sociedad de la información, en la que cada impacto es global y susceptible de ser evaluado a través de una métrica cartesiana, los medios de comunicación tradicionales siguen conservando más alcance que aquellos portales o plataformas de difusión de contenidos que pueden llegar a coquetear con el concepto y la calificación de *fake news* en sus expresiones y sus mensajes.

Es la conclusión que sistemáticamente ha venido alcanzando el Instituto Reuters en países de nuestro entorno como Francia o Italia. No solo la credibilidad es mayor en los primeros casos, sino que son estos los que registran un mayor tiempo de permanencia para las audiencias. Y aun así, hay una segunda cara de la moneda: estos distribuidores de materiales (con frecuencia averiados) obtienen un número mucho mayor de interacciones que los *mass media* que históricamente han conformado el *mainstream*, produciéndose esta mezcla de efecto cascada y en red a través de: a) comentarios a las noticias; b) *posts* compartidos, y c) reacciones de los usuarios de otra índole[1].

¿Es tan masivo y, sobre todo, influyente el alcance de las *fake news* como suele darse por sentado a través de prejuicios u observaciones acientíficas que han calado en la opinión pública con carácter general? Es un hecho que las redes sociales terminan por recoger y hacer cristalizar un flujo de datos constante, inabarcable, imposible de verificar en su totalidad. Pero hay una segunda cuestión medular: ¿puede la *inteligencia artificial* llevar a cabo el trabajo, a través de la creación de algoritmos, de identificar las intoxicaciones que traen causa del denominado *periodismo ciudadano*?

La pregunta no es menor en la medida en que no solo las *fake news* tienden a echarse a rodar ladera abajo instituyéndose en una bola de nieve que engorda incesantemente con riesgos directos y daños colaterales múltiples y serios. Además, producen especialmente debate, polémica, polaridad, posiciones extremas. ¿Cómo alcanzar a señalar si el origen de un mensaje está en un robot? ¿Cómo descubrir si el original está programado? ¿Cómo identificar cuentas similares con acciones semejantes? ¿Cómo dejar al descubierto, uno por uno, aquellos seguidores que han podido ser comprados en la red social? ¿Sería viable disponer de una máquina que chequease un millón de noticias por hora lanzando un aviso inmediato sobre las que carecen de apego al principio de veracidad y, por tanto, parar el golpe antes de su conversión en *trending topic*?

Que la Unión Europea esté sopesando la opción de que estas plataformas sean obligadas a contratar editores humanos que comprueben la autenticidad de las informaciones no es un planteamiento en absoluto inmotivado o

[1] Kleis, Rasmus; Graves, Lucas. «News you don't believe: Audience perspective on *Fake news*», en *Reuters Institute*. Octubre 2017.

caprichoso. Que estudie multas a aquellas webs que reproduzcan contenidos sin contrastar, tampoco. Todos los derechos y libertades fundamentales, en su ejercicio pleno, presentan sus límites, y estos tienen su fundamento ético y jurídico.

La sociedad de la información se ha transformado paulatinamente en una jungla en la que personas sin cualificación, sin formación o sin instrucción pueden erigirse en *influencers* durante horas o días con efectos devastadores, colocándose en la privilegiada posición de actores con capacidad para producir materiales caseros y colgarlos en la Red para obtener un impacto político que puede superar al de los medios convencionales, aprovechándose de un escenario de «desintermediación», en el que los ciudadanos son a la vez productores y consumidores, objetos y sujetos, proveedores y usuarios: un mundo sin los clásicos *gatekeepers* o cancerberos de las esencias del interés general.

Hoy es historia la comunicación en la que la emisión procedía de una o pocas fuentes y se vehiculaba hacia muchos receptores con escasa interactividad. Se han multiplicado los focos productivos: el envío de mensajes a una multitud en la que la estampa final es la de una selva en la que todos los «animales comunicativos» emiten y reciben simultáneamente; la *conectividad* genera automáticamente *sociabilidad* y opera en un marco, esencialmente, de *horizontalidad*.

¿Se trata en su espíritu y su plasmación de una revolución tecnológica que trasciende la pura técnica? ¿Puede haber en esta forma de ciberactivismo una raíz asociada a la profunda crisis de legitimidad de las instituciones políticas y representativas en numerosos Estados del mundo desarrollado?

Es evidente que el ciberespacio ha potenciado la capacidad táctica de ciertos actores preexistentes en los entornos operativos tradicionales, y que ha establecido un ecosistema favorable que ha conllevado la génesis y aparición de nuevos agentes y grupos de presión con capacidades relevantes. Y es evidente que el carácter viral y global de las redes sociales no solo ha actuado como altavoz de la información y la propaganda: está representando una amenaza a considerar para la seguridad y la defensa de organizaciones privadas y Estados. ¿Están desplegando, especialmente estos últimos, las políticas preventivas y reactivas adecuadas y útiles en tiempo y forma?

Repensando el concepto de interés nacional

El debate sobre la afectación de las *fake news* a las políticas de seguridad de los Estados y, por consiguiente, a su propia defensa, tiene pleno sentido, y va ligado a lo que sigue significando el interés nacional en pleno siglo XXI y en una sociedad internacional tan formidablemente globalizada en tantos aspectos, especialmente el de la comunicación y los transportes.

El interés nacional es una noción fundamentada básicamente en el símbolo jurídico del Estado nación, y es esencial para comprender el mundo en que vivimos. Desde que Tucídides por primera vez refirió que una identidad de interés es el más seguro de los vínculos entre Estados e individuos, se ha entendido el alcance, con el paso de los siglos, de lo que significa y en lo que se traduce la «razón de Estado»: la transformación de los intereses personales y particulares en una razón común entre individuos apoyada en una estructura política que será el Estado[2].

El cardenal Richelieu elaboró una concepción moderna del concepto de gobernar, no desde la perspectiva de los intereses particulares del gobernante, sino de los generales de la nación. Y esa idea sigue vigente. También la de Maquiavelo, al considerar que la supervivencia del Estado debe ser la principal preocupación y misión de los dirigentes, convirtiéndose en un fin en sí misma.

El paso de los siglos, y la sociedad actual tan influida por el relativismo y la relajación de ciertas normas éticas, ha visto cómo se ha ido derritiendo el sentido de «razón de Estado» equivaliendo a un «bien moral», el que deriva de la unidad de organización política; pero el papel del Estado como actor catalizador del Gobierno en la sociedad global sigue siendo hoy vital.

Atrás ha quedado, en los desvanes de la obsolescencia, la idea de Kenneth Waltz, según la cual el interés nacional se traduce en la lucha por la supervivencia de los Estados, en un entorno donde no hay autoridad supranacional que regule de forma efectiva sus relaciones. Sin embargo, sigue siendo la necesidad y el deseo de seguridad (traducida esta también en términos económicos) la que conduce a los Estados a intentar sumar y acumular cada día poder, incluyendo el que deriva de la posesión de la mejor información.

La influencia de los principios de la economía de mercado en los postulados liberales asociados al mínimo Estado es innegable, y ha dado lugar a una sociedad donde la defensa a ultranza de las fronteras clásicas ha perdido buena parte de su sentido. Así, los Estados que han intentado gestionar sus recursos y manejar sus potencialidades en clave de interés nacional no han dejado de apartarse de los poderosos motores de crecimiento de la economía mundial con el subsiguiente perjuicio. Hoy mismo es un riesgo, al menos a evaluar desde el plano teórico y en una fase embrionaria de los Estados Unidos de Donald Trump.

No hay interés nacional sin seguridad nacional. Y en la relación entre el primero y la segunda opera indefectiblemente la información: su cantidad, su calidad, su relevancia, su especificidad, su naturaleza... Un Gobierno que no disponga de la información adecuada, o que no evalúe adecuadamente aquella a la que pueda acceder, y que adopte decisiones contra su seguridad

[2] AAVV. *Evolución del concepto de Interés Nacional*, Monografías del CESEDEN, 2010.

nacional fracasará en la defensa de sus intereses: tanto los estratégicos e inmutables como los de coyuntura o pasajeros.

Una sociedad en la que el problema puede venir derivado no de la falta de información sino del exceso de la misma provoca que el Estado se enfrente a nuevos desafíos desde el punto de vista del análisis de riesgos y amenazas. Aquellos y estas obligan al desarrollo de nuevas estrategias y tácticas, de nuevos métodos para la extracción de información potable para la generación de inteligencia, con el fin último de disponer de la preparación necesaria y suficiente para enfrentar escenarios imprevistos.

En un mundo sacudido y convulsionado por el concepto de *posverdad*, los Estados se enfrentan a ciertas ecuaciones para la salvaguarda y la promoción de esos intereses nacionales que permanecen casi inalterables. En primera instancia, la definición de aquellos intereses compartidos (y no compartidos) con otros actores; en segundo término, la definición de los riesgos a los que se está sometido y el grado de cobertura necesario para su protección, y en tercer lugar, la concreción y materialización de los medios materiales y morales disponibles para incluir en la Estrategia de Seguridad Nacional. Esto ha significado y significa contemplar la tecnología y las posibilidades de financiarla y acoplarla a los mecanismos para la consecución de los objetivos establecidos, empezando por la defensa de la integridad, de la independencia y de la soberanía nacional.

Por encima de este enfoque, que tiene un componente de tradición y permanencia en el tiempo, carece de sentido omitir que los Estados, en la defensa de su propio interés nacional, se enfrentan hoy a fenómenos globales que propician riesgos y amenazas que están trastocando su propia fisonomía y que agravan o multiplican sus efectos. Entre ellos, las disfunciones de la propia globalización que, con frecuencia, se traducen en: a) desequilibrios demográficos; b) pobreza y desigualdad; c) cambio climático; d) peligros tecnológicos, y e) ideologías radicales y no democráticas.

Se trata, en su conjunto, de tendencias de largo alcance y estructurales con una inmensa fuerza para provocar desórdenes e inestabilidad en el sistema internacional. Y ello en un escenario en el que los Estados no constituyen (como antaño o como anteriormente los imperios) las únicas fuentes de poder: de un lado, porque una parte de su soberanía es cedida voluntariamente a cambio de beneficios acordados de la más diversa especie; de otro, porque la propia globalización ha facilitado que empresas multinacionales, e incluso organizaciones no gubernamentales, hayan podido erigirse en auténticos poderes transnacionales que compiten con los Estados para condicionar la política, la economía y algunos aspectos de la propia seguridad internacional.

El teatro de la *posverdad* afecta además de forma muy notable a los denominados *Estados fallidos* o *Estados frágiles*, aquellos que tienen una especial y grave dificultad o incapacidad para preservar y ejercer el monopolio legítimo de la fuerza, asegurar el respeto a la ley, aportar seguridad física a su pobla-

ción o suministrarle unos servicios públicos mínimos; aquellos que padecen conflictos armados prolongados, colapso institucional, abusos y enfrentamientos sectarios o a organizaciones de carácter tribal.

Y la afección no viene determinada siempre o únicamente (pensemos, por ejemplo, en Irak) por el hecho de que unidades insurgentes tengan acceso a las últimas herramientas tecnológicas y las exploten para la propalación de propaganda o falsedades. Viene, en parte, porque las *fake news* fabricadas desde las sociedades más económicamente desarrolladas (Estados Unidos, Europa y otras), que aluden a fenómenos ocurridos en los citados *Estados frágiles*, pueden condicionar las políticas que llevan a la práctica los Gobiernos de las primeras respecto del territorio de los segundos.

Aún más. Que Estados que operan bajo el paraguas, por ejemplo, de la OTAN sean incapaces de controlar los bulos (incluso en forma de campaña) que se difunden desde sus fronteras, puede terminar provocando que esos *Estados fallidos* objeto de la desinformación vean agravada su situación, produzcan un añadido de desestabilización sobre sus vecinos y contagien de incertidumbre a regiones enteras.

Hacia una transición en los modelos de seguridad

Toda guerra de información se sustancia en la distribución de datos o relatos intencionadamente manipulados al servicio de ciertos fines, o en ocasiones se basa en la aportación de información insuficiente o directamente en su omisión. No se trata, por tanto, de divulgar simples mentiras, sino de mensajes tanto verdaderos como falsos para producir el efecto del engaño en los receptores. El objetivo no es otro que el de desacreditar y debilitar a los oponentes, distorsionar así su percepción de la realidad, y, en ese sentido, se trata de una operación que se incardina de lleno en el ámbito de la defensa.

Cualquier modelo de seguridad por el que se apueste, y cualquier política que de él derive, busca identificar y gestionar los posibles riesgos para impedir que dañen los intereses fundamentales de cualquier comunidad, representada políticamente por un Estado o por un conjunto de ellos, como es el caso de la Unión Europea o la OTAN.

Es un planteamiento invariable, más allá de que el marco estratégico en el que se deba articular la estrategia de seguridad y defensa se vea afectado por nuevos fenómenos (¿coyunturales, estructurales?) como los que traen causa de todo lo que significa el universo de la *posverdad* en el campo de la información y las nuevas tecnologías.

Hoy han quedado completamente superados los modelos que parten de la base y argumentan que las relaciones internacionales solo se entablan entre Estados, y que por consiguiente las amenazas y los riesgos tienen carácter exclusiva o preponderantemente militar. Esta concepción, resultado de uno

de los paradigmas del realismo político que identificaba el principal foco de los estudios de seguridad con el fenómeno de la guerra, ha quedado desbordada —décadas atrás— por la proliferación y la diversificación de los actores con capacidad para acumular y ejercer el poder en la sociedad internacional. Aún más, ni siquiera hoy puede colegirse que la política exterior solo exista entre Estados nación soberanos, en la medida en que estos no son los únicos que disponen de capacidad para ejercer la coacción sobre terceros actores y, así, moldear el orden internacional.

Sobre el papel, la globalización de las comunicaciones induce al aterrizaje en un marco estratégico muy influido por el idealismo y por la configuración de una amplia comunidad (en realidad todos los habitantes del planeta) conectada, con relaciones esencialmente cooperativas y con las barreras entre los pueblos (no solo las fronteras físicas) derribadas o ausentes.

Sin embargo, y a pesar de que existan por añadidura reglas comunes e instituciones que limiten los conflictos, a pesar de que existan en la sociedad global ciertos valores comunes reconocidos y aceptados, el empuje de las *fake news* ha introducido en el ecosistema informativo internacional una idea de descontrol, de anarquía, de cierto caos. ¿Es posible contenerlo o revertirlo?

El hecho es que este fenómeno particular y el contexto más amplio definido como *posverdad* se lee mejor si cabe a la luz de la doctrina elaborada al finalizar la guerra Fría por los autores agrupados en la escuela de Copenhague. En términos históricos recientes, apenas hace tres décadas, ya cobra fuerza el dibujo de un nuevo concepto de seguridad en el que los riesgos y las amenazas incluían, sin ningún género de dudas, fenómenos de carácter no tradicional.

Así, la tendencia que cobra cuerpo y vigor es la de un grupo de *amenazas no militares* a la seguridad, tremendamente heterogéneas, que pasan al primer plano y que se concretan en hechos incontestables como el subdesarrollo, la corrupción, el derroche de los recursos o las violaciones de los derechos humanos, entre otros. Y esta amalgama provoca que al Estado nación, en su gestión, se unan otros actores del sistema (no estatales) u organizaciones regionales.

Desde este prisma, y en el interior de este encuadre, la apuesta por un marco de *seguridad colectiva* ha basculado a otro de *seguridad compartida*[3]. Así, si la sociedad internacional contemplaba de forma más rotunda e inmediata un compromiso de acción, incluso armada, contra el infractor que ponía en peligro la paz y la seguridad, hoy procura desechar la idea prioritaria del uso de la fuerza haciendo hincapié en herramientas ligadas a la confianza y la cooperación.

[3] Calduch, Rafael, *Dinámica de la Sociedad Internacional*, Madrid: Ceura, 1993.

La era de la *posverdad* se configura como un espacio de tiempo en el que la gestión de los desafíos se produce de forma más interdependiente y con un mayor énfasis en las actuaciones responsables y eficaces, y en el que, desde espacios territoriales como la Unión Europea, se diseñan estrategias globales para mantener un estatus de libertad y prosperidad, combatiendo fenómenos como el terrorismo, abordando cuestiones capitales como las que resultan de la ciberseguridad y contemplando en primer término aspectos vitales que conciernen, por citar un caso, a la seguridad en los suministros energéticos.

También esta era pone en el primerísimo orden el concepto de *resiliencia*[4], entendida como la capacidad de los Estados y las sociedades para reformarse, soportando situaciones adversas extremas (incluidos los desastres) y gozando de fuerte impulso para superar las crisis internas y externas. Y, por añadidura, coloca nuevas responsabilidades sobre las organizaciones de las que esos Estados son parte.

En el caso de la Unión Europea, la redefinición de su estrategia de seguridad recoge una visión estructurada en varios parámetros sobre los que acometer una inversión incesante y colectiva.

De un lado, se subraya la necesidad de exhibir *credibilidad*, siendo necesario en este sentido un desarrollo pleno de todas las herramientas de la política exterior, desde la investigación hasta la lucha contra el cambio climático, pasando por las infraestructuras, la movilidad, el comercio, la diplomacia y el desarrollo. De otro, se enfatiza la oportunidad de disponer de *rapidez en la respuesta*, de acuerdo a la velocidad a la que se producen los cambios, y esto flexibilizando y ajustando las decisiones a las prioridades y los objetivos de forma exigente y permanente. Por último, se pone el acento en la *imagen de integración*, tan útil en todos los ámbitos para trasladar una percepción de coherencia y, por consiguiente, de solvencia.

En el caso de España, el fin de la seguridad nacional se configura como un estado a alcanzar a través de la acción y de una serie de principios de actuación en los que cobra progresivamente más sentido:

a) La *anticipación*, que implica disponer de los medios necesarios para alertar y prevenir de todos aquellos elementos que puedan poner en peligro la seguridad nacional.

b) La *interdependencia responsable*, que supone contribuir a la creación y el fortalecimiento de marcos e instrumentos multilaterales (con socios europeos e internacionales) que garanticen la seguridad.

c) El *enfoque integral*, que se plasma a través de la implicación, coordinación y armonización de todos los organismos, actores y recursos del

[4] De Carlos, Javier. «Tendencias Globales, Seguridad y Resiliencia», en *IEEE*, Documento de Investigación. Junio 2017.

Estado para hacerlos converger en la consecución de los objetivos fijados en el sistema de seguridad.

d) La *resiliencia*, que se manifiesta en la capacidad de resistencia y recuperación mediante instrumentos flexibles, susceptibles de adaptarse a las más diversas circunstancias y de sobreponerse a las situaciones de crisis, minimizando y absorbiendo sus consecuencias negativas.

Nuevos horizontes de la cultura de defensa

Difícilmente puede llevarse a cabo un análisis pormenorizado y profundo de las derivadas que la era de la *posverdad* conlleva en términos de seguridad nacional si no se delimita de dónde viene y hacia dónde va la *cultura de defensa*. Y esta no puede sino entenderse como un conjunto de conocimientos, normas, valores, metas, actitudes y prácticas compartidas socialmente y orientadas a proteger y garantizar los intereses nacionales. En definitiva: un proyecto compartido.

El punto de salida del que debe partir el análisis sobre la evolución de la cultura de defensa en los nuevos parámetros que marcan la sociedad global de la información y el conocimiento es: ¿cuáles son los motivos que justifican la necesidad de seguir fomentando esa idea apenas naciente en su concepción moderna?

De un lado, parece positivo que se haga preciso generar conciencia sobre la utilidad de percatarse de la importancia de las cuestiones relativas a la seguridad nacional en todas sus dimensiones. De otro, parece positivo que se haga útil asumir una serie de deberes y obligaciones respecto a la seguridad nacional.

Esta segunda causa, interpretada con cierto sesgo ideológico, puede ser desvirtuada al hacerse equivaler al imperativo de construir algún tipo de espíritu grupal de signo patriótico. Pero no es ese su fundamento ni su meta. La referencia es clara, y está dirigida a los beneficios colectivos que son consecuencia del hecho de que todos los sectores sociales y el conjunto de la ciudadanía conozcan las principales amenazas y riesgos a los que se exponen, así como las formas de actuación que el Estado trata de llevar a cabo para atajarlos, con el mayor grado de transparencia de las organizaciones dedicadas a facilitar seguridad.

Un proyecto de cultura de defensa exitoso no puede sino fomentar el sentido cívico y de corresponsabilidad, favorecer la percepción general de protección, ampliar la confianza y el prestigio social de las Fuerzas Armadas para otorgar más legitimidad a la tarea que desempeñan y concienciar incluso sobre el uso responsable de todos los recursos que ofrece Internet.

En este sentido, la información, la comunicación y la *participación de todos* en la *seguridad de todos* no puede sino derivar en un grado más elevado de co-

hesión donde del compromiso solidario se desprenden mejores resultados en la acción.

La seguridad (siendo en términos absolutos inalcanzable), especialmente en democracia, es la garantía de la construcción y consecución de otros fines. Es el mejor paraguas para la salvaguarda de los derechos fundamentales y las libertades públicas. Por tanto, la cultura de defensa puede y debe promover no el planteamiento de que el ciudadano ha de sacrificar hasta perder derechos y libertades para estar seguro, sino, muy por el contrario, el foco de que el ciudadano habrá de disponer de seguridad para poder ejercitar en toda su plenitud sus derechos y libertades, empezando por aquellos que nacen en su ámbito más íntimo, privado y personal.

Son las sociedades abiertas los entornos con más ventajas para que quienes las conforman, civilmente, entiendan la relación inversamente proporcional entre seguridad y riesgo: a mayor grado de consecución de la primera, menos presencia del segundo, y viceversa. Y son las sociedades abiertas los marcos idóneos para que se pueda desarrollar una auténtica conciencia sobre el hecho de que: a) hay amenazas que provienen de agentes hostiles; b) hay bienes que se deben proteger, determinando en primera instancia aquellos esenciales, y c) hay una cobertura, mecanismos que deben articularse para alcanzar la seguridad.

La permanente transformación de la naturaleza de las amenazas ha provocado una readaptación constante de las prioridades de la política exterior y de defensa en todo el planeta. Hoy la seguridad humana se busca defendiendo más personas que territorios, y eso implica, en muchos casos, defender como bienes el propio Estado del bienestar con los derechos y libertades que lleva aparejados y que resultan de un proceso acumulativo de conquistas históricas y colectivas, ya irrenunciables.

Por lo que respecta a las guerras de información, es incontrovertible que la naturaleza misma del conflicto bélico no ha cambiado desde el inicio de los tiempos, pero los medios y modos de afrontarlo no han dejado de virar. Hoy, la democratización de los avances tecnológicos y determinadas facilidades de acceso, sumado este factor a la proliferación de adversarios con conocimientos para convertir en armas esas herramientas, está propiciando cambios cualitativos y viscerales en los tradicionales paradigmas de confrontación. Ese cambio viene determinado, sobremanera, por el empleo de medios de comunicación digital y de redes sociales como arietes para producir hostilidad (en ocasiones, en insufribles cantidades industriales).

La Inteligencia: ayer, hoy y mañana

La sociedad del conocimiento en la que el concepto de *posverdad* ha irrumpido fuertemente, deslizándose por numerosas vertientes, se configura como un sistema complejo en el que la inteligencia, como ha ocurrido histórica-

mente pero hoy de forma más acentuada, está llamada a jugar un papel de primera magnitud.

La inteligencia, tanto la humana como la propia de los servicios secretos de los Estados y las corporaciones privadas, combina la dotación de significado a la realidad con la anticipación ante esa realidad. Así, Estado y empresa disponen de inteligencia cuando usan aquella que obtienen y almacenan para construir un significado propio de su realidad, la de su organización y su entorno.

Ese conocimiento es usado para adoptar decisiones sobre el futuro: gestionando el riesgo, anticipando amenazas (también oportunidades) y, en el mejor de los casos, actuando sobre el momento para conformar posibles futuribles donde la organización fomente ventajas competitivas.

Las amenazas y oportunidades que más sorprenden, con un alto impacto en un país, suelen tener origen en sectores no conocidos o no explotados. Establecer un sistema de inteligencia exige dedicar medios para conseguir unos retornos que se percibe llegarán no inmediatamente, sino a medio y largo plazo. Por consiguiente, la seguridad está relacionada de forma directa con la inteligencia y la vigilancia.

Pero incluso en el mundo de las *fake news*, de la intoxicación difundida masivamente a través de campañas en redes sociales y otros medios tecnológicos, la utilización de la inteligencia no ha supuesto un cambio. Se ha transformado la cultura informacional como recurso intangible, la supervisión de los cambios en el entorno, la circulación del conocimiento en redes.

También el espionaje está variando sensiblemente las coordenadas en que se desarrolla, sin mutar su esencial naturaleza. Sigue siendo una actividad perpetrada conscientemente para penetrar en un espacio informacional protegido o descuidado, a fin de conseguir un incremento de conocimiento por medios encubiertos, insospechados o desconocidos por su legítimo propietario. Sigue siendo esa actividad con la que se busca información protegida bajo diferentes niveles de clasificación y de accesibilidad muy limitada, cuyo contenido es sensible y de alto valor para el conocimiento de capacidades e intenciones de un enemigo, e incluso de un aliado.

Hoy, en plena ola de democratización y expansión casi ilimitada en el uso de nuevas tecnologías, se está incrementando el riesgo de accesos no permitidos y robos de esta información que ponen contra las cuerdas a su legítimo dueño y le generan vulnerabilidad. No solo el robo de información secreta militar, sino industrial, económico-financiera o de índole política.

En efecto, el signo de los tiempos ha conllevado al auge del espionaje digital, una modalidad de ciberataque directamente instigado contra la confidencialidad de los datos en la que el uso de «armas de información» se lleva a cabo para alcanzar un acceso no autorizado a redes, sistemas y repositorios electrónicos considerados de interés estratégico para, por ejemplo, un Estado.

Es este marco el que impone a las organizaciones volcar sus esfuerzos con especial énfasis en distintos ámbitos y con distintos objetivos: el primero, el de alcanzar la independencia tecnológica a través de la búsqueda de la autonomía en el desarrollo e implantación de soluciones y dispositivos para alcanzar niveles óptimos de seguridad de datos; el segundo, el de elevar al máximo nivel la protección de información sensible, desarrollando políticas de defensa eficaces al cortocircuitar eventuales agresiones, y el tercero, el de reforzar la propia función y las capacidades de los equipos de respuesta a emergencias informáticas para garantizar una óptima gestión de la calidad en seguridad de la información[5].

Proteger hoy el conocimiento significa hacerlo no solo sobre el contenido sino sobre los propios canales por los que discurre desde su generación hasta su explotación final, y de los propios departamentos en los que se almacena o recopila; significa que las empresas que lo producen con aplicaciones a la innovación industrial deben mantenerlo con frecuencia en secreto para salvaguardar su posición en un contexto internacional competitivo, pudiendo generar así valor añadido.

En una sociedad de la información en la que es creciente el número de actores que queda públicamente expuesto, perder información repercute, además de económicamente, en la pérdida de reputación de la organización atacada en el ciberespacio. Y este riesgo es permanente y alto en la medida en que cada día grupos más pequeños trabajan en modo mercenario en todo el mundo en la cancha del ciberespionaje.

Y aun así, la era de la *posverdad* y de la *deep web* sigue siendo la era de la sobreabundancia de fuentes abiertas. En este sentido, sería imprudente —a cualquier efecto de captación, análisis y explotación de información— ignorar la que fluye a través de las redes sociales, ya sea por desconocimiento o por infravaloración. Al contrario: puede resultar decisiva para completar y redondear el ciclo de inteligencia.

Por esta razón, dos de las principales amenazas del uso de datos provenientes de las redes sociales como fuente de investigación son la información falsa y la *infoxicación*. Por Internet fluyen todo tipo de contenidos sin filtrar, salvo en países determinados en donde se aplica censura, y eso implica que el celo debe extremarse en la valoración del mensaje y la fuente. Del mismo modo, por las redes fluye el ruido inútil que dificulta la obtención de información realmente relevante, y el uso deliberado y sistemático de las nuevas tecnologías (de este magma) en modo campaña puede movilizar rápidamente a millones de personas, con los problemas de seguridad que ello puede generar.

[5] Díaz Matey, Gustavo. *Los servicios de inteligencia ante el siglo xxi*, Ediciones Chavín, 2011, pp. 167-190.

Un hándicap para Estados y organizaciones económicas con fuertes aparatos de inteligencia es la imposibilidad de controlar la herramienta. Las redes se encuentran en manos de grandes corporaciones que definen sus propios objetivos y necesidades[6] y que operan sin considerar el inmenso daño social que pueden producir conglomerados o individuos antisistema que, simplemente, difunden su ideología, realizan captación de nuevos miembros, explican su agenda o ejercen influencia[7].

Dados estos parámetros, ¿no resulta hoy imprescindible como nunca que la propia sociedad civil adquiera una cierta *cultura de inteligencia* y que lo haga a través de una mecánica de sensibilización pública que mejore el conocimiento por parte de los ciudadanos de los fines y las funciones de sus servicios de información como institución que forma parte del Estado democrático y que actúa al amparo de la legislación y es controlado por esta?

El arma de doble filo de las TIC

Internet y el resto de Tecnologías de la Información y la Comunicación han determinado, y lo siguen haciendo, importantísimos cambios sociales, y han llevado al primer plano la ciberseguridad como conjunto de herramientas, políticas, conceptos y salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas y seguros que pueden utilizarse para proteger los activos de la organización y a los usuarios en el ciberentorno.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los servicios o aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en ese ciberentorno, y la seguridad vuelve a ser aquí crucial, el concepto clave, para entender la inevitabilidad de trabajar en la protección de eventuales agresiones.

Los ataques 3.0 pueden perjudicar y perjudican hoy a sistemas complejos, golpeando a individuos, a la propia sociedad civil, a empresas y a los Estados. Los *malware* (códigos maliciosos capaces de actuar de forma inadvertida) pueden operar hoy sobre cualquier ordenador, y los programas espía tienen capacidad para recabar información sobre cualquier entidad, comprendiendo datos personales del espiado, sus acciones en el ciberespacio, los contenidos de su disco duro o las características de sus conexiones.

Hay más: programas de suplantación de identidad (*pishing*) distribuidos a través de correo electrónico, idénticos a la correspondencia enviada por or-

[6] Pintado Rodríguez, César, «Las redes sociales y la defensa. Un análisis DAFO», en IEEE, Documento de Opinión. 119/2013.

[7] Aún así, plataformas como Facebook, en casos extremos han actuado clausurando a, por ejemplo, grupos yihadistas o bandas de neonazis entregados a la apología del racismo.

ganizaciones bancarias o marcas legales y que incluyen enlaces que redireccionan a páginas falsas desde las que se absorben datos confidenciales. O, en el caso de los *adwares*, accesos a publicidad camuflados en programas que recopilan y envían datos confidenciales del usuario sin su conocimiento.

En una era supeditada sobremanera al uso de las nuevas tecnologías, la ciberguerra (las operaciones orientadas a penetrar sin autorización los ordenadores y sistemas o redes de información de algún Estado con el propósito de perjudicarle) marca el signo de los tiempos.

Alterar, perturbar o impedir el funcionamiento de los equipos informáticos afectados o de los objetos que están controlados por dichos equipos, dañar los datos en ellos contenidos o introducir información falsa conforman una galería de acciones incluidas en la caja de herramientas de toda suerte de malhechores. No solo se trata de actuaciones cibernéticas de apoyo a operaciones bélicas convencionales en el marco de misiones militares, sino de aquellas que se implementan exclusivamente en el ciberespacio, de forma autónoma e independiente.

Precisamente, en la medida en que los ciberataques se erigen en una de las amenazas más peligrosas y con mayores posibilidades de desarrollo a corto plazo, cualquier estrategia de seguridad nacional debe tener hoy como objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, comenzando por la gestión de las infraestructuras críticas del Estado[8].

Estas últimas se encuentran, vía grupos subversivos que operan en el ciberespacio, en la parte más alta de su lista de objetivos por las averías económicas que puede producir su destrucción o interrupción y por su virtualidad de garantizar la fiabilidad de las redes de abastecimiento del gas, de sistemas de transporte, de distribución de petróleo o del propio tendido eléctrico.

La metamorfosis en los procesos de comunicación

La comunicación es una de las herramientas en las que se apoya la legitimidad de acción de cualquier persona con deberes y responsabilidad de actuación en el campo de lo público. Una buena comunicación contribuye a la transparencia, a generar confianza y a rendir cuentas ante la ciudadanía. Pero en el ámbito de la seguridad, por la convicción de que compartir información debilita y hace vulnerable, suele prodigarse la incomunicación y el secreto; por consiguiente, la opacidad.

En efecto, el ámbito de la defensa presenta una serie de singularidades (muchas de ellas obvias) que invitan e imponen restricciones en ocasiones in-

[8] EFE, «España superará los 700 ciberataques en infraestructuras estratégicas en 2017», 6 de junio de 2017.

eludibles a la difusión de datos y mensajes. De hecho, el exceso informativo en este campo: a) produce el efecto perverso de brindar conocimiento a los actores generadores de amenazas y, por tanto, les allana su camino para causar daños, y b) puede contribuir al pánico social, en la medida en que la sensación ciudadana de seguridad e inseguridad es subjetiva: la primera crece lentamente, la segunda se dispara exponencialmente.

Hoy, como en el inicio de los tiempos, la información es expresión de poder. El mandato representativo en democracia tiene fuerza cuando el ciudadano se siente protegido en sus intereses, depositando su alícuota parte de poder en unos representantes que van a velar por él. La ocultación de información puede provocar una ficticia sensación de seguridad, porque los riesgos y las amenazas siguen ahí.

En la era de la *posverdad*, la globalización económica y cultural corre paralela a la globalización de las amenazas, que no solo son transnacionales sino extraestatales, como el ciberterrorismo y el crimen organizado con medios tecnológicos. Algunos de los actores que practican estas formas de violencia (sea con fines políticos o crematísticos) buscan con frecuencia un impacto mediático, y eso significa que la comunicación no solo es relevante para las instituciones oficiales de poder, también es crucial para quienes pretenden revertir los patrones de seguridad estatal.

Aún más. En la era de las *fake news*, los grandes medios de comunicación de masas siguen sirviendo de canal fundamental para alcanzar vastas audiencias, pero han proliferado los conductos que hacen posible evitar su mediación para copar la atención de los ciudadanos. Eso se traduce en que se ha ensanchado el terreno de juego para expandir rumores, para confundir la conciencia colectiva mediante la duda, para crear estados de incertidumbre política y social, para malograr debates de interés general... o para desestabilizar y provocar cambios de tendencia en los procesos electorales.

En ese espacio en el que confluyen la política y la seguridad se está detectando la capacidad de actores que pueden jugar en favor de la fortaleza de un partido o un régimen, que pueden aumentar artificialmente la popularidad de un candidato o un líder, que pueden hacer invisible a un contrincante destruyendo su reputación o que pueden ahogar las críticas a autoridades, sistemas políticos o estructuras del Estado[9].

Especialmente en el ámbito de la seguridad y la defensa, por su dimensión estratégica, los mensajes emitidos por las instituciones han de ser consistentes y coherentes. Cualquier tipo de incongruencia (por apariencia pequeña que tenga en tamaño) termina por erosionar la imagen de la institución, y esos mensajes deben contemplar las «líneas rojas» que dejan al margen del discurso público por pura necesidad, lo que se debe ocultar. Una técnica

[9] Pintado Rodríguez, César. «Las redes sociales...», art. cit.

—la de la ocultación— nada fácil de aplicar, con criterios perfectamente definibles y explicables por sus potentes implicaciones éticas y profesionales.

En efecto, la gestión de la información en el área de la defensa adquiere una dimensión trascendente. A partir de su contenido, su forma y el medio por el que se transmite se configuran las percepciones en la calle. Y el gran problema al que se enfrentan las estructuras de seguridad interior es qué comunicar y cómo hacerlo cumpliendo con los criterios de transparencia que incesantemente empujan desde todas las direcciones imaginables.

Un escenario de audiencias volátiles y empoderadas

La multiplicación de actores con capacidad de comunicar e influir en la era de la *posverdad* ha dejado obsoletos ciertos modelos con los que se pretendía explicar la dinámica, la razón de ser y los efectos del ecosistema informativo, tanto a nivel nacional como internacional.

De acuerdo a los modelos de élite dominantes, como el de «propaganda o fabricación del consenso» de Herman y Chomsky[10], los medios son simples instrumentos del sistema capitalista y de quienes lo controlan y trabajan por su supervivencia. En el modelo «indexado» de Bennett[11], el discurso político de quienes dominan la vida económica de la sociedad se reproduce y amplifica, produciéndose solamente debates muy debilitados en casos de disenso entre las élites.

La democratización y expansión de las nuevas tecnologías ha propiciado, sin embargo, que se hayan abandonado esas formulaciones fundamentadas en audiencias pasivas y *mass media* actuando unidireccionalmente. Así, la opinión pública alcanza hoy la misma importancia que el resto de sujetos comunicativos, al ser sus percepciones y valoraciones capaces de modificar la diplomacia, los conflictos y las políticas de seguridad y defensa. Los medios tradicionales se sitúan, en consecuencia, en una ubicación intermedia: sin ser instrumentos propagandísticos del Gobierno o el Estado ni tampoco adversarios abiertos.

Aun así, en el caso de Europa y de España, encontramos la irrupción reciente, en las dos últimas décadas, de televisiones como Hispan TV o Russia Today, que han roto ciertos esquemas de la percepción de las audiencias y las han sometido a encuadres nuevos y sesgados sobre temas complejos, como el

[10] Pedro, Joan, «Evaluación crítica del modelo de propaganda de Herman y Chomsky», en *Revista Latina de Comunicación Social*, n.º 64, 2009.

[11] Moreno, José Manuel, «La importancia de los encuadres en la política exterior y los nuevos desafíos comunicativos», en *Análisis GESI, 33/2017*.

conflicto palestino-israelí o los conflictos de Afganistán, Siria o Ucrania, llegando a facilitar informaciones de dudoso origen y veracidad[12].

El fenómeno no es baladí, especialmente considerando que los efectos sobre las audiencias en cuestiones de política exterior son pronunciados: la opinión pública, en términos generales, carece de convicciones ideológicas y posicionamientos fuertes, y dispone de un reducido nivel de conocimiento de temas, como regla, de pronunciada profundidad.

Precisamente por eso, el poder de Internet y, por tanto, de las redes sociales, pudo provocar (en clave de instrumento de movilización) las revueltas de 2011 de la llamada Primavera Árabe, que terminaron por derrocar los Gobiernos de Túnez, Egipto y Libia. En efecto, de forma impactante e imprevisible, el uso de las herramientas cibernéticas desató una tormenta de efectos estratégicos y duraderos, condicionando el inicio, el desarrollo y el enlace de esas revueltas y esos conflictos. La propia democratización de la Red ha tenido una influencia directa sobre la reestructuración de la cobertura de los conflictos armados, al fracturarse el monopolio ejercido por los medios tradicionales. El caso emblemático de la CNN y de su cobertura de la guerra de Irak, con la presencia estelar de Peter Arnett, ha quedado relegado al baúl de los recuerdos[13].

La aparición de blogs y portales de noticias alternativos ha terminado por configurar un entorno diferente, competitivo, en el que quedan mitigados (cuando no anulados) los procesos de *gatekeeping*, generándose un contexto mucho más volátil e inseguro. La propia propagación de bulos o noticias de difícil confirmación ha terminado por afectar colateralmente (y de manera en cierto modo paradójica) a los viejos medios, deteriorando su imagen profesional ante lectores y espectadores.

Injerencias imprevistas en procesos electorales

Los *hackers* se han convertido en actores invisibles que pueden influir e influyen en los procesos electorales de medio mundo. Es un hecho este que replantea preguntas sobre el uso de las nuevas tecnologías en las sociedades democráticas. Y esta circunstancia debe unirse al hecho de que las redes sociales están debilitando algunas de las condiciones que históricamente han posibilitado la existencia de Estados nacionales democráticos: ¿cómo es posible que millones de votantes reciban por sistema noticias falsas promovidas en la generalidad de los comicios que celebran las primeras democracias del planeta?

---

[12] Ruiz De La Serna, Ricardo. «La infuencia de Irán en España», en *Libertad Digital*. 21 enero 2016.

[13] Valenzuela, Javier. «CNN se despide de su reportero estrella, Peter Arnett, tras un reportaje falso», en *El País,* 20 abril 1999.

La era de la *posverdad* conduce a una reflexión de vastas dimensiones. El sentimiento de cohesión que los ciudadanos de las naciones modernas han sentido tradicionalmente entre sí (el grado en el que podían considerarse parte de una comunidad nacional) estaba en gran medida facilitado por la función que cumplían los medios de comunicación de masas. Ahí queda el célebre aforismo de Arthur Miller: «A *good newspaper is a nation talking to itself*».

Los sistemas de gobierno democráticos han dependido en un grado u otro de ese sentimiento compartido de comunidad que incluso ha posibilitado *políticas de Estado* que nacen de la idea de que los ciudadanos hacen converger sus intereses y convicciones ineludiblemente en un puñado de cuestiones decisivas.

En el pasado, las sociedades han dependido de *intermediarios de los intereses generales*, por lo general periodistas, para enmarcar y articular ese sentimiento de realidad compartida. Hoy, las personas reciben fundamentalmente el tipo de información que ellas mismas han seleccionado y configurado previamente o (más temerario) que terceras partes han decidido que les interesa conocer.

Este coctel desinformativo explosivo para la democracia se ha cruzado con el fenómeno del hackeo electoral. Los protagonistas de estos delitos han vulnerado los sistemas de comunicación de figuras políticas, de partidos y de parlamentos. Han vulnerado la integridad y han manchado la limpieza de procesos para favorecer a unos candidatos o programas sobre otros. Y así se entiende el *doxing*, procedimiento selectivo y estratégico implementado con el ánimo de inclinar la balanza electoral de uno de los lados.

Pero hay mecanismos de contaminación más sigilosos y perversos. En la era de la *posverdad* las opiniones políticas son más proclives a polarizarse. ¿Por qué? Por razones que emanan de tiempos pretéritos, de la vicisitud en la que un votante se ve obligado a decantarse por una u otra propuesta. Pero hoy esas tendencias son exacerbadas, a más abundamiento, por los algoritmos de las redes sociales que conducen al usuario, inexorablemente y con presencia de motores predictivos y de *inteligencia artificial*, hacia informaciones que coinciden con sus preestablecidas preferencias. ¿Acaso no debilita cada *news feed* la deliberación democrática para radicalizar las convicciones propias e intransferibles?

Y, aun así, el Estado democrático y social de derecho se enfrenta a fórmulas más agresivas de injerencia en campaña. Es la que se vincula a la usurpación de identidades, al *hacking* de registros electorales y a la propia intervención de los resultados, haciendo inseguros los escrutinios. Es la razón por la que se ha estimulado inevitablemente el levantamiento de barreras tecnológicas (algunas apoyadas en la criptografía, incluso el *blockchain*) para blindar los comicios.

Indiscutiblemente, solo el diseño arquitectónico de una nueva gobernanza cibernética internacional permitirá evitar una crisis de confianza generalizada y global de los ciudadanos frente a las instituciones democráticas[14].

Realidades y mitos de las operaciones rusas

En términos generales, los Gobiernos de distintos Estados (incluido España) han sido extremadamente cautos al evitar atribuir a Moscú la autoría de las noticias falsas que han inundado cíclicamente las redes sociales en momentos sensibles, como procesos electorales o crisis internas de diversa naturaleza. Y eso, a pesar de que una y otra vez se ha constatado que porcentajes altísimos (en ocasiones superando el 50%) de los perfiles que han difundido *fake news* procedían de servidores alojados en territorio ruso.

Para la opinión pública y el *mainstream* de las naciones europeas y Estados Unidos, ha quedado suficientemente acreditado no obstante que Rusia ha intervenido activamente en medios y redes por medio de mecanismos de propagación de noticias falsas en todos los procesos políticos de relevancia occidentales en los últimos años, incluyendo el proceso independentista catalán y el referéndum a favor del Brexit en Reino Unido.

El hecho es que no resiste a la discusión que, como en el caso de otras naciones, para la Federación Rusa la desinformación es un método militar asimétrico e indirecto en los modernos espectros de guerra híbrida, y es, por consiguiente, un instrumento principal en su estrategia de influencia geopolítica.

Como otras naciones, la rusa ha manejado como medidas activas en la guerra de información la propaganda, la provocación o la manipulación de los medios de comunicación extranjeros. Desde Lenin, la militarización de la información ha sido habitual en una estrategia que ha pivotado sobre la influencia, no en la fuerza bruta, siendo su objetivo trascendental romper la coherencia interna del sistema político, económico y militar del enemigo, no aniquilarle.

Esa guerra informativa tenía y tiene como medios «adoctrinar» a la población para desestabilizar la sociedad y forzar a los Estados a tomar decisiones favorables a los intereses de sus oponentes. Desde las propias Fuerzas Armadas Rusas se ha señalado que lo que más distingue la guerra convencional de la híbrida es la simultaneidad en esta de las batallas en tierra, mar, aire y espacio informativo, y el uso de métodos indirectos y no lineales para alcanzar objetivos militares[15].

[14] Santiso, Carlos; Dahan, Mariana. «Cómo protegemos nuestras democracias en la era digital», en *El País*. 23 agosto 2017.

[15] Milosevich, Mira. «La "combinación", instrumento de la guerra de información de Rusia en Cataluña», en *Análisis del Real Instituto Elcano*. 7 noviembre 2017.

En la última década, tanto en los planos oficial como oficioso, Rusia ha trabajado de manera constante y activa para imponer «un punto de vista alternativo» en la óptica de los ciudadanos (principalmente, pero no solo) de Europa y Estados Unidos. ¿Por qué?

A la Federación Rusa le ha beneficiado difundir globalmente el mensaje de que su poder está bajo permanente lupa y amenaza de un Occidente hegemónico y decadente que aspira a excluirla del orden internacional. En el caso de la Unión Europea, al tratarse de una entidad política al borde del colapso y la desintegración, incapaz de solucionar sus múltiples crisis; en el caso de la OTAN, al funcionar como una organización desgastada y sin horizonte ya, con riesgo de provocar la Tercera Guerra Mundial por su afán infundado de expandirse hacia las fronteras del Este.

Así, ha convenido la difusión de contenidos (no solo noticias) que han perseguido poner en evidencia la disfuncionalidad del sistema político, económico y social de la democracia liberal, creando confusión y sembrando dudas, favoreciendo las diferencias o la desunión de los miembros de instituciones adversarias, transmitiendo que ni la integración continental es el camino más seguro hacia la prosperidad ni el movimiento de construcción europeo es irreversible[16]; esa percepción ha alimentado a los partidos populistas y continentales extremistas ubicados tanto en la derecha como en la izquierda.

La guerra de información/desinformación alentada desde Moscú no solo ha ido encaminada a generar un marco en el que se propalan noticias de dudosa veracidad, sino a poner el foco sobre la figura de *agentes independientes*, activistas antiglobalización o militantes de diversas causas fuertemente ideologizados y radicalizados para elevar la voz en favor de causas que, de algún modo, sirven a los objetivos de poder de Rusia: uno de ellos, crear divisiones para minar progresivamente la fortaleza de Europa y sus propios instrumentos y mecanismos de respuesta ante diversas coyunturas.

El hecho es que una galería de medios prorrusos no solo han hecho campañas encubiertas a favor del Brexit, Marine Le Pen y la ultraderecha alemana; igualmente, han mantenido una línea editorial sin contemplaciones al matiz y alineada con el punto de vista de Moscú sobre la guerra en Siria, las provocaciones de Corea del Norte o la presidencia de Donald Trump.

En definitiva, en la era de la *posverdad* los medios prorrusos han identificado los flancos más vulnerables de Europa y sus crisis (moneda única, Estado del bienestar, inmigración/refugiados) para desacreditar todo un modelo de principios y valores, de desarrollo. ¿Están activados los mecanismos de defensa para responder a estas novísimas agresiones sin viso de ser flor casual de un día?

16 Ibídem, s.p.

Conclusiones: cómo detener a atacantes invisibles

En la era de la *posverdad*, en la que se persigue movilizar y hacer prevalecer las emociones por encima de la realidad y el rigor de los hechos, toda estrategia de seguridad nacional deberá partir del diagnóstico de que las campañas de desinformación forman parte de planes más amplios y ambiciosos de desestabilizar a un oponente, por lo general un actor estatal.

La viralización automática y global de mensajes engañosos a través de perfiles programados o robots está disparando exponencialmente una amenaza ya de primera magnitud. En el origen está el hecho de que los medios de comunicación tradicionales han perdido el monopolio y el control de los flujos de información transnacionales y, a pasos agigantados, se dejan por el camino la notoriedad, la influencia y la publicidad. Hasta tal punto de que un candidato como Donald Trump llegó a ser presidente de la primera potencia mundial no solo viviendo de espaldas a las corrientes de opinión que generaban (contrarias a sus intereses), sino declarándoles «enemigos del pueblo» y calificándoles despectivamente, como hiciera su consejero Steve Bannon, de «principal partido de la oposición».

La preponderancia de la comunicación sobre la propia información se ha convertido en un factor fundamental de riesgo y susceptible de ser explotado para producir inestabilidad. Esencialmente, en la medida en que la acción comunicativa no plantea una búsqueda de la verdad (obligación que sí contempla la actividad informativa).

Carecerá de sentido, por insuficiente, cualquier política de seguridad que no identifique las redes sociales como lugares para poner en contacto a personas con ánimo hostil y dañino que pueden socavar, en un momento determinado, intereses nacionales a través de campañas de manipulación masiva. Más si cabe en un ecosistema posmoderno en el que, más allá de la esencia de los actos, se imponen los distintos tipos de narración sobre los mismos y, por tanto, la diversidad de percepciones producidas.

Cualquier estrategia futura de defensa tendrá que partir del desafío vital de identificar operaciones de engaño. Con la multiplicación de emisores se ha disparado la dificultad para averiguar la exactitud de lo contado y de comprobar la credibilidad de las fuentes. Es la moneda de cambio cotidiana en un mundo en el que los hechos objetivos se remiten a la trastienda, presentándose en el frontispicio de lo comunicable y lo noticiable el universo de las creencias personales y, aún más revolucionario, las simples emociones.

El daño producido por las *fake news* que originen reacciones en cadena de puro desconcierto entre los ciudadanos (a veces millones) será incalculable no solo si no se articulan políticas de seguridad y defensa efecti-

vas y acordes a la idiosincrasia de la amenaza, sino, por añadidura, si no se planifican acciones de alfabetización digital que doten a la sociedad civil de mecanismos de defensa frente a la intoxicación y la mentira. El pensamiento crítico vuelve a ser el patrimonio y el arma más codiciada, y más escasa.