

AMBITO COGNITIVO Y SEGURIDAD NACIONAL: UNA PERSPECTIVA DE SEGURIDAD INTERIOR

RAFAEL JOSÉ DE ESPONA

ACADÉMICO CORRESPONDIENTE – REAL ACADEMIA DE JURISPRUDENCIA Y
LEGISLACIÓN DE ESPAÑA

Fecha de recepción: 01/09/2022 Fecha de aceptación: 17/11/2022

RESUMEN

Las implicaciones del devenir del Ámbito Cognitivo para la Seguridad Interior son múltiples. La reciente mención específica del Ámbito Cognitivo considerado como uno de los concretos campos de la acción de la Seguridad Nacional se recoge en la *Estrategia de Seguridad Nacional 2021*. Al igual que los ámbitos físico y cibernético son objeto de la acción protectora de la acción de Seguridad Interior, lo mismo acontece respecto del Ámbito Cognitivo. Se presenta como principal reto la adecuada delimitación jurídico-constitucional de una función de acción cognitiva de seguridad que tiene a su disposición tecnologías de elevada potencia invasiva, bajo un riguroso cumplimiento normativo de índole garantista. La acción protectora del Ámbito Cognitivo por parte de los organismos competentes en materia de Seguridad Interior requiere la adecuada capacidad funcional para la oportuna vigilancia y, en su caso, intervención, comportando la salvaguarda de los Derechos y Libertades Fundamentales.

Palabras clave: Ámbito Cognitivo, Seguridad Nacional, Seguridad Interior, Libertades y Derechos Fundamentales, Ingeniería Social.

ABSTRACT

There are several implications of dynamics of the Cognitive Domain regarding Homeland Security. The recent specific mention of the Cognitive Domain considered as one of the concrete fields for National Security action is included in the *National Security Strategy 2021*. As far as the physical and cybernetic domains are the object of the protective action of Homeland Security, the same happens concerning the Cognitive Domain. It seems the principal challenge the right legal-constitutional framing of the cognitive function security action, that has high-invasive technologies, according to a strict rightly-based legal compliance. The protective action of the Cognitive Domain by competent public institutions on Homeland Security issues needs the accurated functional ability for the timely surveillance and, when applicable, intervention, including the safeguard of Fundamental Freedoms and Rights

Keywords: Cognitive Domain, National Security, Homeland Security, Fundamental Freedoms and Rights, Social Engineering.

1. INTRODUCCIÓN

El Ámbito Cognitivo ha existido siempre como una de las dimensiones de la realidad humana, si bien la moderna proliferación de las tecnologías de información y telecomunicaciones (TICs) a escala global y con un alcance capilar a toda la población, conlleva que su estructura se haya configurado de manera compleja y que su dinámica sea vertiginosa. La reciente mención específica del Ámbito Cognitivo considerado como uno de los campos de la acción de la Seguridad Nacional se recoge en la *Estrategia de Seguridad Nacional 2021*, habiendo sido precedida por la Publicación Doctrinal Conjunta del Estado Mayor de la Defensa *Doctrina para el Empleo de las FAS*, (PDC-01 EMAD 2018).

Las implicaciones del devenir del Ámbito Cognitivo para la Seguridad Interior son múltiples. Se requiere, ante todo, una adecuada comprensión del citado ámbito, su estructura y componentes, así como de las metodologías que se emplean para las tareas de vigilancia e intervención sobre aquel. Así mismo, es imprescindible un conocimiento disciplinar de la problemática de la epistemología y de las neurociencias en general -conjugando los aspectos teóricos de sus postulados junto con su proyección funcional en la práctica- así como una visión completa sobre el estado del arte de las tecnologías aplicadas -disponibles tanto de manera comercialmente accesible para el sector civil, como reservada para actividades de seguridad o defensa- para poder orientar la acción de los Cuerpos y Fuerzas de Seguridad del Estado sobre el Ámbito Cognitivo.

Al igual que los ámbitos físico y cibernético son objeto de la acción protectora de la acción de Seguridad Interior, lo mismo acontece respecto del Ámbito Cognitivo. Se presenta como principal reto de esta tarea la adecuada delimitación jurídico-constitucional de una función de acción cognitiva que tiene a su disposición tecnologías de elevada potencia invasiva. Ello requiere -bajo un riguroso cumplimiento normativo de índole garantista- equilibrar la discrecionalidad administrativa (con especial consideración al principio auto-contención operativa) con la acción protectora del Ámbito Cognitivo por parte de los organismos competentes en materia de Seguridad Interior -sin perder la perspectiva de conjunto del marco del *Sistema de Seguridad Nacional*- con especial hincapié en la salvaguarda de los Derechos y Libertades Fundamentales.

La perspectiva de Seguridad Interior sobre el Ámbito Cognitivo se encuentra de inicio un contexto de desregulación y paradigmas normativos obsoletos ante un estado del arte de las neurociencias y las TICs altamente sofisticado y dinámico -el cual ha impactado en las estructuras sociales alterando múltiples paradigmas epistemológicos sobre la política, la organicidad social y la economía, según ha estudiado González¹- con la

1 GONZÁLEZ, Wenceslao. J., "Tipos de diseño, innovaciones democráticas y relaciones internacionales", en ESTANY, A. y GENSOLLEN, M. (eds), *Diseño institucional e innovaciones democráticas*, Eximia-Universidad Autónoma de Barcelona-Universidad Autónoma de Aguascalientes, Barcelona, en prensa. GONZÁLEZ, Wenceslao. J., "From Intelligence to Rationality of Minds and Machines in Contemporary Society: The Sciences of Design and the Role of Information", *Minds and Machines*, v. 27, n. 3, (2017), pp. 397-424. DOI: 10.1007/s11023-017-9439-0. GONZÁLEZ, Wenceslao. J., "Internet en su vertiente científica: Predicción y prescripción ante la complejidad", *Artefactos: Revista de Estudios de la Ciencia y la Tecnología*, v. 7, n. 2, (2018), 2ª época, pp. 75-97. GONZÁLEZ, Wenceslao. J., "Complejidad dinámica en Internet como plataforma de información y comunicación: Análisis filosófico desde la perspectiva de Ciencias de Diseño y el papel de la predicción", *Informação e Sociedade: Estudos*, v. 28, n. 1, (2018), pp. 155-168. GONZÁLEZ, Wenceslao. J., "Internet y Economía: Análisis de una relación multivariada en el contexto de la complejidad", *Energeia: Revista internacional de Filosofía y Epistemología de las Ciencias Económicas*, v. 6, n. 6, (2019), pp. 11-36. GONZÁLEZ, Wenceslao. J., "La dimensión social de Internet: Análisis filosófico-metodológico desde la complejidad", *Artefactos: Revista de Estudios de la Ciencia y la Tecnología*, v. 9, n. 1, (2020), 2ª época, pp. 101-129.

necesidad de paliar las lagunas normativas mediante el recurso a la analogía con los ámbitos físico y cibernético. Existe una clara superioridad de medios privados de acción cognitiva con gran potencial desestabilizador y de capacidad agresiva (a diferencia de lo que acontece en los casos de las armas o *software* para la acción cinética o cibernética, respectivamente, contrastando la inferioridad de medios en el sector privado respecto del público)². Ante este panorama, no parece desencaminado argüir que los Cuerpos y Fuerzas de Seguridad del Estado están necesitados de una conceptualización, doctrina y medios actualizados para desenvolver sus misiones en el Ámbito Cognitivo.

Es propósito del presente estudio señalar la necesidad de dotar de una adecuada capacidad funcional a los organismos competentes en Seguridad Interior, para la oportuna vigilancia y, en su caso, intervención sobre el Ámbito Cognitivo, en el contexto del Sistema de Seguridad Nacional de España, para la protección de la población española, sus libertades y derechos fundamentales.

2. EL ÁMBITO COGNITIVO COMO DIMENSIÓN DE LA SEGURIDAD NACIONAL

La delimitación específica del Ámbito Cognitivo como una de las dimensiones de la acción de la Seguridad Nacional ha sido reflejada en distintas publicaciones oficiales, destacando la *Estrategia de Seguridad Nacional 2021* -habiéndose sido precedida por la PDC-01 del JEMAD en 2018³- la cual refiere a dicho ámbito (p.60) junto con el señalamiento de los problemas de desinformación creciente, las injerencias digitales, el contexto de amenazas híbridas y la importancia de la lucha contra la desinformación (pp. 81, 82, 83), apuntando a la elaboración de una Estrategia Nacional de Lucha contra las Campañas de Desinformación (p. 83)⁴.

Partiendo de la consideración del Ámbito Cognitivo como una dimensión intangible inherente al ser humano, considerada de forma individual, socializada u organizada, que es consustancial a su capacidad de juicio y de toma de decisiones y que alcanza a las voluntades de todas las personas, aquel impregna al resto de ámbitos, físico y cibernético. Para operar en el Ámbito Cognitivo, se manejan aspectos inmateriales y de difícil ponderación, incluyendo valores, percepciones, emociones, conciencia, actitudes y prejuicios. Se actúa sobre él mediante el empleo de técnicas de comunicación, la neurociencia aplicada, la psicología, sociología y otras disciplinas sociales como la denominada Ingeniería Social (explicada por AVERY en base al concepto de Popper)⁵. A diferencia de los ámbitos físico y cibernético, el cognitivo es totalmente inasible en sentido material. Al mismo tiempo, la interrelación de este con los demás ámbitos -especialmente el cibernético⁶- ha de ser tenida permanentemente presente, para la debida coherencia operativa.

2 NATO STRATCOM CoE-SINGULAREX, "The Black Market for Social Media Manipulation", NATO Strategic Communications Centre of Excellence, Riga, 2018.

3 EMAD, Publicación Doctrinal Conjunta PDC-01 (A) *Doctrina para el empleo de las FAS*, Estado Mayor de la Defensa, 2018.

4 DSN, *Estrategia de Seguridad Nacional 2021*, Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

5 AVERY, Thomas, "Popper on "Social Engineering": A Classical Liberal View", *Reason Papers*, vol. 26 (2000) pp.29-38.

6 La guía *Desinformación en el ciberespacio* del CCN-CERT incide en la estrecha relación entre el ciberespacio y el Ámbito Cognitivo. CCN-CERT, *Desinformación en el ciberespacio*, CCN-CERT / BP 13, febrero 2019. Asimismo, el problema se explica en LEWIS, James A., "Cognitive Effect and State Conflict in Cyberspace", CSIS, 2018.

El Ámbito Cognitivo contemporáneo se caracteriza por la accesibilidad masiva de la tecnología aplicada a las telecomunicaciones y a la gestión de información, la superabundancia informativa y de canales de difusión y terminales individuales de recepción al alcance de la masa social, la llamada Sociedad de la Información. Esta se perfila por cinco factores: saturación y desatención, empleo de metodologías analíticas irreflexivas, premisas epistemológicas implícitas simples, difusión de información asociada a Ingeniería Social, y soporte electrónico creciente con una constante digitalización de procesos y proliferación de las denominadas *Internet de las cosas (IoT)*⁷ e *Internet de los cuerpos (IoB)*⁸.

En la sociedad, debido a la superabundancia de información disponible y a la alta frecuencia de difusión de nuevos contenidos, las audiencias están desbordadas, produciéndose una congestión informativa y una desatención por sobrecarga de estímulo. Así, la percepción se debilita al producirse una desatención sobre la información o, aún captándola, no se asimila en su totalidad o en su adecuado sentido. La manera en la que la información se percibe depende en gran parte de la forma en la que se procesa (y reside también en el tipo de procesos de análisis empleados en el proceso intelectual consciente reflexivo o inconsciente intuitivo). Las premisas epistemológicas implícitas simples refuerzan este factor descrito, y las categorías de pensamiento -conceptos predeterminados, dogmática científica, paradigmas y tópicos culturales- operan como premisas que condicionan el procesamiento de la información en todo su recorrido.

Entre la *niebla* suscitada por el “ruido informativo”, se vislumbra la difusión de información asociada a vectores de Ingeniería Social. En la relación entre sociedad e información, opera un vector de doble sentido: aquella genera información y también la recibe. En este orden, las aportaciones informativas al Ámbito Cognitivo son susceptibles de modelar la sociedad en términos metodológicos de ingeniería (en tanto sean configuradas adecuadamente en sus contenidos/silencios, forma de exposición, canales de difusión y cronología). Debido a las distintas capacidades, percepción y estructura social de la población y de las élites (con una capacidad decisoria de muy distinto alcance, y que son disímiles en el orden político, científico, religioso, cultural y económico), las técnicas de Ingeniería Social y la instrumentalización de la información serán diferentes, aunque operando en un plano común⁹.

Toda esta fenomenología que ha conformado singulares parámetros estructurales en la sociedad industrial -y una novedosa dinámica práctica del devenir del Ámbito Cognitivo contemporáneo en tanto se enmarca en aquella- no es ajena a los distintos actores estatales o privados, aliados o enemigos, terroristas, criminales o

7 Acrónimo de la expresión inglesa *Internet of Things*.

8 Acrónimo de la expresión inglesa *Internet of Bodies*. LEE, Mary Lee, BOUDREAUX, Benjamin, CHATURVEDI, Ritika, ROMANOSKY, Sasha, DOWING, Bryce, *The Internet of Bodies. Opportunities, Risks, and Governance*, RAND, Santa Monica, 2020, pp.23ss. SILBERGLITT, Richard, ANTON, Philip S., HOWELL, David R., WONG, Anny, GASSMAN, Natalie, JACKSON, Brian A., LANDREE, Eric, PFLEEGER, Shari Lawrence, NEWTON, Elaine M. , WU, Felicia, *The Global Technology Revolution 2020, In-Depth Analyses. Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, RAND, Santa Monica, 2006, p. xix.

9 Véase el recientemente constituido foro contra la Desinformación: <https://www.dsn.gob.es/es/actualidad/sala-prensa/creaci%C3%B3n-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-> ; y la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

simplemente activistas, que intervienen sobre dicho ámbito generando nuevas situaciones, problemáticas, amenazas y retos a la Seguridad Nacional. La acción cognitiva negativa (criminal, terrorista o análoga) tiene a su alcance técnicas depuradas de Ingeniería Social hostil capaz de desestabilizar y/o influir a la población (siendo incluso capaz de integrar una “narrativa implícita” en las interpretaciones difundidas sobre las propias acciones agresivas, de manera que se condiciona una percepción empática favorable a las mismas), modificando parámetros sociales y generando efectos muy lesivos contra la Seguridad Nacional.

Por lo tanto, desde la perspectiva de la Seguridad Interior, el Ámbito Cognitivo requiere una adecuada protección frente a vectores negativos de carácter activista radical hostil, delincencial, criminal, subversivo o terrorista (además del reto de la Guerra Cognitiva y de las múltiples modalidades de Operaciones Psicológicas¹⁰). Análogamente a como acontece en los ámbitos Físico y Cibernético, el cognitivo requiere su propia salvaguarda desde las Administraciones Públicas, siendo una precondition la adecuada vigilancia y monitorización del mismo. El Ámbito Cognitivo siempre estará ocupado por vectores de acción cognitiva convencional (i.e. medios de comunicación, propaganda comercial, difusión cultural, libre expresión de la ciudadanía), incluyendo aquellos generados por distintos actores que son en buena parte inciertos, desde los cuales -por principio de prudencia- debe suponerse se pueden pretender realiza acciones cuando menos divergentes de los efectos deseados por los poderes públicos nacionales.

La capacidad de Alerta Temprana y respuesta rápida respecto de amenazas o acciones hostiles en el Ámbito Cognitivo se dificulta por la confusión que las rodea y sus concurrencias multi-dominio (especialmente cibernético, pero también físico). La complejidad de las tareas de identificación, clasificación (según su complejidad taxonómica), seguimiento e interdicción (y, en su caso, implementación de contra-medidas), de dichos vectores cognitivos, requiere contar con las capacidades adecuadas. Por esta razón, es imprescindible una conciencia situacional permanente, anticipada al ataque y con capacidades prospectivas y de Alerta Temprana en el Ámbito Cognitivo.

Se entiende como Vulnerabilidad Cognitiva el grado de perjuicio y sensibilidad al daño procedente de impactos negativos de índole cognitivo, en el más amplio sentido, abarcando desde el condicionamiento y la desestabilización (cuya sutileza redunda frecuentemente en mayor eficacia¹¹) hasta la coerción destructiva. La exposición en el Ámbito Cognitivo (en el que se encuentra inmerso, de una u otra manera, el conjunto

10 U.S. ARMY, *From PSYOP to MindWar: The Psychology of Victory* by Colonel Paul E. Vallely, Commander, with Major Michael A. Aquino, PSYOP Research & Analysis Team Leader, Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, CA, 1980. ARONHIME, Lawrence Aronhime, COCRON, Alexander (sup.), *Countering cognitive warfare: awareness and resilience*, Johns Hopkins University & Imperial College London, 20 May 2021. KRISHNAN, Armin, “From Psyops to Neurowar: What are the Dangers?”, ISAC-ISSS Conference, Austin, November 2014. MOUTON, Francois, PILLAY, K., VAN’T WOUT, M.C., “The Technological Evolution of Psychological Operations Throughout History”, en: Clarke, N.I., Furnell S.M. (editors), *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2016 Frankfurt), ed. Plymouth University, Plymouth, 2016, pp.266-278. SIBONI, Gabi, “The First Cognitive War”, en: Kurz, A., Brom, S (eds.), *Strategic Survey for Israel 2016-2017*, Institute for National Security Studies, Tel Aviv, 2016.

11 ESPONA, Rafael José de, “Seguridad energética y guerra psicológica”, Instituto Español de Estudios Estratégicos (en línea), Documento de Opinión 66/2016, 1 de julio de 2016.

de la población) comporta la susceptibilidad a verse influido por el mismo, según las condiciones subjetivas del sujeto pasivo. En tanto que este tenga un determinado grado de sensibilidad, dicha influencia cursará con desigual alcance. Si existen condiciones de vulnerabilidad en el sujeto o colectivo del que forma parte (*cluster* social o audiencia), se multiplicará la magnitud del potencial impacto ante un vector cognitivo, y ello tendrá un nivel de riesgo cognitivo mayor en función de aquella.

3. ACOTACIÓN Y ESTRUCTURACIÓN DEL ÁMBITO COGNITIVO

El conjunto de la población interacciona constantemente con el Ámbito Cognitivo, el cual se conforma precisamente por la inter-vinculación de las mentes de sus componentes. Las personas se relacionan a través de redes de intercomunicación personal (sea esta una comunicación meramente humana entre individuos, o bien sea canalizada y potenciada por medios -físicos o telemáticos- de transmisión o difusión de información). Ello acontece en un doble sentido: activamente, por las aportaciones vertidas en el Ámbito Cognitivo desde la iniciativa humana; pasivamente, por la recepción vía comunicación directa o impregnación informacional que repercute en toda mente humana expuesta a dicho ámbito. La población conforma la denominada Opinión Pública o tendencia dominante de estados de opinión.

La configuración de la estructura social -sus segmentos, *clusters* y elementos definidos por distintos criterios de clasificación- conlleva una correlativa conformación del Ámbito Cognitivo; en el seno de este último se encuentran unos mecanismos de modulación del Ámbito, así como una determinada proyección y recepción de sus efectos. En este sentido, respecto de la nación propia, se delimita lo que cabe denominar como Ámbito Cognitivo connacional o interior no en un sentido físico-territorial -pues el espectro cognitivo es intrínsecamente poroso y transfronterizo- aunque psicológicamente se ve acotado por los esquemas mentales de la población por la idea de territorialidad, soberanía y arquitectura institucional del Estado. A ello se añaden las limitaciones a la transmisibilidad de información (obstáculos a la emisión o a la difusión) y las barreras de percepción (idiomáticas, culturales, idiosincrásicas y análogas). No obstante la no-territorialidad del Ámbito Cognitivo, cabe dirigir la acción institucional sobre el mismo en un sentido competencial que lo delimite de manera coincidente con el territorio de soberanía, en tanto en cuanto los cauces de difusión de los vectores cognitivos se circunscriben al espacio terrestre y aéreo propio y la audiencia objetivo máxima es la población connacional o residente en este.

Para que las dinámicas sociales cursen en un contexto cognitivo de libertad, se requiere la impregnación de todo el Ámbito Cognitivo de los principios que sustenten unas interrelaciones en el seno del mismo debidamente protegidas frente a potenciales injerencias, empleo abusivo de medios de difusión, distorsión deliberada e influencia perniciosa, superando la mera persecución del delito.

Aunque el Ámbito Cognitivo siempre ha existido en todo colectivo humano, el crecimiento exponencial de los medios de generación de contenidos de impacto cognitivo, telecomunicación y difusión en tiempo real de información ha conformado un entorno de la información caracterizado por la saturación, junto con una desatención por parte de la población, tanto cualitativa (dificultad para detectar la información de calidad y pérdida de capacidad intelectual para procesarla e interpretar correctamente, para alcanzar un

grado de conocimiento adecuado) como cuantitativa (la mente humana está ampliamente desbordada en cuanto a la cantidad de información disponible). En este último sentido, la proliferación -entre gran parte de la población, incluyendo sectores ilustrados- de premisas epistemológicas y de una dinámica analítica empobrecidas, incide negativamente en sus capacidades de percepción e interpretación.

La dinámica de información y desinformación es inherente al conocimiento humano, incluso sin intencionalidad alguna. La cuestión de la desinformación es compleja en cuanto a su definición, pues existen errores de interpretación y transmisión, rumores infundados por alteración de la cadena de transmisión informativa, debates académicos, polemología científica y discrepancias de criterios técnicos en todo tipo de materias y disciplinas, alcanzando también a la propia información de carácter oficial o dimanante de las Administraciones Públicas. La existencia de tendenciosidad deliberada, maliciosidad intencionada, finalidades negativas subrepticias o cualesquier inteligencia coordinadora oculta que instrumentalice el juego de información-desinformación. Por ello, resulta esencial poder interpretar correctamente la estructura y dinámica del Ámbito Cognitivo para discernir contenidos y vectores espontáneos, bienintencionados o de tendenciosidad contenida y no negativa, de aquellos que evidencian acciones de influencia hostil, modelación e Ingeniería Social invasivas sobre la población (total o segmentada, o sobre élites y tomadores de decisión), perjudicial para el equilibrio y estabilidad social, y el mantenimiento de Libertades y Derechos Fundamentales sobre el Ámbito Cognitivo.

Si bien no cualquier contenido informativo, vector cognitivo u operación (de publicidad, *marketing*, concienciación, activismo, cultural, ideológica, etc.) implementada en el Ámbito Cognitivo es susceptible de calificarse como amenaza o agresión cognitiva o de finalidad delictiva, siempre incidirá -en alguna medida, incluso involuntariamente- en el campo de la Seguridad Interior, aunque sea como factor de contexto.

3.1. CENTROS DE GRAVEDAD

El carácter etéreo del Ámbito Cognitivo dificulta su delimitación y la identificación de sus elementos principales, de manera que para analizarlo y actuar sobre él procede ante todo señalar sus Centros de Gravedad (COGs¹²). Los COGs del Ámbito Cognitivo son áreas específicas y acotadas de este, sobre los que pivota el conjunto de todos los elementos que lo componen. Constituyen puntos centrales de generación y creación de contenidos que son la base de narrativas o sus premisas epistemológicas rectoras, y de vectores cognitivos de máxima influencia.

Estos COGs están compuestos fundamentalmente por personas¹³ vinculadas entre sí por elementos cognitivos (identidad de pensamiento o nexo epistemológico) sin perjuicio de otros enlaces que pueden ser concurrentes (i.e. familiares, tribales, institucionales, económicos, etc.). Sobre ellos se identifican los caracteres, vectores cognitivos (y agentes) asociados, canales de comunicación-difusión e instrumentos

12 Acrónimo de su denominación inglesa *Centers of Gravity*.

13 Conviene no confundir el concepto de Centro de Gravedad del Ámbito Cognitivo con el elemento organizacional humano o entidad institucionalizada que acoge o enmarca dicho COG pues, aunque sean concurrentes o uno se subsuma en el otro, pertenecen a ámbitos y son elementos heterogéneos, contemplándose analíticamente los COGs en cuanto a sus contenidos, vectorización y efectos.

en el Ámbito Físico y en el Ámbito Cibernético con los que se correlacionan ¹⁴. Ante todo, los COGs del Ámbito Cognitivo han de ser analizados partiendo de la comprensión de su propia estructura informativa y proyección cognitiva, con sus contenidos informativos inherentes, siendo interpretados cotejando las distintas percepciones internas y externas que generan.

3.2. VECTORES

Los contenidos y el entorno de la información en el Ámbito Cognitivo operan dinámicamente a través de lo que podemos denominar Vector Cognitivo, el cual es un elemento informativo coherente, intencionado, concordante y confluyente en un efecto común, de manera que conforma un módulo con dirección y sentido definido en el contexto del Ámbito Cognitivo.

Utilizando la analogía conceptual con el término vectorial empleado en Física (definido como segmento de recta, contado a partir de un punto del espacio, cuya longitud representa a escala una magnitud, en una dirección determinada y en uno de sus sentidos), con el empleo figurativo de los Vectores Cognitivos podemos describir las distintas dinámicas y su carga material a lo largo del Ámbito Cognitivo, junto con sus orientaciones, coordenadas de origen e intensidad.

Cabe distinguir un abanico de tipología de vectores cognitivos -en función de su taxonomía empleando distintos criterios de clasificación, que podemos sintetizar fundamentalmente en función de su origen, actor, contenido, canal difusor, finalidad y grado de agresividad/hostilidad.

Todo Vector Cognitivo es susceptible de ser contrarrestado con un vector opuesto, así como es posible introducir otros vectores concurrentes que supongan una dilución de sus efectos (preventiva o reactivamente), o bien que neutralicen sus bases (narrativa) mediante una contra-narrativa o narrativa complementaria modificadora.

Habida cuenta la dependencia de los Vectores Cognitivos de la narrativa inherente y de la actitud condicionadora de la percepción por parte de las audiencias, aquellos son proclives a su instrumentación, re-direccionamiento o reconversión en nuevos vectores, mutando su configuración y alterando sus efectos previstos.

Cabe actuar sobre los vectores provocando su atenuación o intensificación mediante acciones de refuerzo. Lo primero es especialmente claro en los casos de interés en reducción de la *energía social* sobre un elemento desestabilizador del Ámbito Cognitivo (y, por extensión, de la sociedad y de las instituciones); lo segundo, puede ser útil para generar una distorsión o desgaste por haber producido una hipertrofia del vector que lo hace ineficaz por desproporcionado.

14 La limitación al Ámbito Cibernético es un error conceptual, pues el Ámbito Cognitivo interacciona con el Físico con mayor trascendencia en muchos aspectos. Así, cabe considerar aspectos como la posible infiltración de personal en escuelas de pensamiento, medios *main-stream*, agencias de noticias, productoras y generadores de contenidos informativos o de entretenimiento. Existe un excesivo énfasis sobre el Ámbito Cibernético el cual, aunque permite la máxima velocidad y volumen de datos, no es único ni el prevalente soporte de información en los ámbitos de élite.

3.3. CONTENIDOS

Esencialmente, en los contenidos presentes en el Ámbito Cognitivo -dejando aparte la información desagregada, los datos dispersos y el ruido informativo (espontáneo o deliberado)- la agrupación coherente de la información se estructura en torno a narrativas. La narrativa es una secuenciación coherente de la información que compone un relato (cuya inteligibilidad estará sustentada por unas premisas epistemológicas y una metodología analítica implícita en el receptor), estructurado para favorecer su credibilidad e incidir persuasivamente sobre la audiencia-objetivo. Las narrativas pueden ser de distinta composición, lenguaje conceptual y estilo, mensaje, audiencias-objetivo y efectos potenciales. Del caudal de los contenidos del Ámbito Cognitivo cabe extraer elementos informativos puntuales que son de gran valor cualitativo, los cuales evidencian la estructuración subyacente de aquellos (i.e. partiendo de determinados esquemas mentales o enfocando concretos parámetros de Opinión Pública, etc.) y los vectores cognitivos presentes. Hay también contenidos abstractos, canalizados por estímulos visuales o acústicos, de gran impacto incluso sin narrativa aneja, como la música¹⁵.

3.4. EFECTOS

En términos generales, todo elemento del Ámbito Cognitivo tiene un efecto, en tanto en cuanto su interacción con los contenidos los modifica respecto de su significado y perceptibilidad. En sentido estricto, consideramos los efectos buscados o espontáneos de los contenidos presentes en el Ámbito Cognitivo y, en particular, de los vectores generados con alcance o propósito específico. Así, a cada vector cognitivo le corresponderán una serie de efectos como resultado de su percepción por parte de las audiencias (lo que acontecerá en desigual medida, conforme a la direccionalidad que se haya dirigido hacia unos destinatarios específicos). Por su grado de importancia e intencionalidad, se distinguen distintos tipos de efectos pretendidos sobre el Ámbito Cognitivo, generados a partir del impacto causado por un vector cognitivo. En cuanto a la taxonomía de efectos según el impacto causado, cabe describir un amplio elenco que abarca su carácter positivo o negativo; desde la perspectiva de la protección del Ámbito Cognitivo y de la Seguridad Interior, estos últimos tienen un desglose de múltiples configuraciones respecto de su lesividad, criminalidad o alcance terrorista. La dinámica de información versus desinformación y la retroalimentación que supone el entrechoque e interacción de vectores cognitivos concurrentes o competitivos comporta un entorno informacional mutable. Por todo ello, para asegurar la fiabilidad de las acciones cognitivas respecto de los efectos pretendidos, se requiere un constante re-direccionamiento o generación de nuevos vectores para corregir efectos imprevistos.

3.5. ACTORES

Por su posición dinámica, distinguimos en el Ámbito Cognitivo dos tipos de actores: de un lado, los activos que, en sentido lato, son todos aquellos que aportan contenidos

15 JUSLIN, Patrik, VASTFJALL, Daniel, "Emotional responses to music: The need to consider underlying mechanisms", *Behavioral and Brain Sciences*, n.º 31, 2008, pp. 559-621. LOVEGROVE, Kitty, "The acoustic world on influence: how Musicology illuminates Strategic Communications", *Defence Strategic Communications*, vol. 5, Otoño 2018, pp. 13-49.

y, en sentido estricto, aquellos que generan vectores. En todos ellos, según su organización, grado de sofisticación -roles, intereses, autonomía/concertación, medios humanos/ autómatas (IA, bots)- e intencionalidad, cabe apreciar la existencia de inteligencias coordinadoras¹⁶ y agentes de influencia subyacentes. De otro, los pasivos; genéricamente lo es toda la población expuesta al Ámbito Cognitivo (a su vez, en sentido humano individual, todos actor activo también lo es pasivo); concretamente, lo son las audiencias y *clusters* sociales a las que concretamente van dirigidas las acciones cognitivas y sus vectores (así como los colectivos que realizan tareas de de monitorización analítica (AA. PP.), convirtiéndose en objetivo receptor de las señales que otros colectivos homólogos o confrontados puedan enviarles en su rol activo). Entre el conjunto de los actores pasivos, se distinguen básicamente los vulnerables de los no vulnerables.

3.6. EL PROBLEMA DE LA ATRIBUCIÓN

El principal obstáculo de correlación ente las acciones sobre el Ámbito Cognitivo y su originador activo, es la cuestión de la atribución causal¹⁷, cuestión especialmente dificultosa en cuanto a la prueba legal de la misma, y constitutiva de una forma de cursar el proceso forense compleja que comporta el análisis de metadatos con sofisticadas técnicas. Para una adecuada atribución de toda acción cognitiva, se requiere una definición, rastreo y detección de *inteligencias coordinadoras* subyacentes que aprovechan, parasitan o instrumentalizan vectores cognitivos de generación espontánea y en boga. Se considera Inteligencia Coordinadora al actor organizado, interno o externo, supuesto o incierto, generador de vectores cognitivos e instrumentador de fuerzas sociales, cuya existencia es puesta en evidencia por la estructuración compleja subyacente a los indicadores, señales o vectores cognitivos que permiten inferirlo.

4. MARCO INSTITUCIONAL COMPETENCIAL

La acción de protección sobre el Ámbito Cognitivo ha de estar debidamente enmarcada en el ordenamiento constitucional, partiendo del principio de salvaguarda de las Libertades y Derechos Fundamentales, especialmente en dicho ámbito en este caso. La protección de la estabilidad y libertad social y su capacidad de resiliencia y de seguridad cognitiva es tarea a desarrollar por las AA.PP. propias del Estado de Derecho, propiciando la confianza social en las instituciones. Esto coadyuvará a las actividades de asuntos públicos e información institucional hacia la sociedad. De acuerdo con su marco competencial, los órganos de Seguridad Interior -en el contexto de Seguridad Nacional- asumirán el reto sin perder de vista que la monitorización operativa del Ámbito Cognitivo incide al tiempo en la denominada “zona gris” que puede evidenciar un posible origen militar externo de Amenazas Híbridas. En todo caso, se actuará desde los más rigurosos criterios deontológicos para garantía de la legitimación ética de la acción institucional de protección -sea de vigilancia o de intervención- sobre el Ámbito Cognitivo.

16 La invasión rusa de Ucrania ha ido acompañada de intensas acciones cognitivas lanzadas desde organismos rusos, crecientemente desde 2014. VV.AA., *Rivalry in the Information Sphere. Russian Conceptions of Information Confrontation*, RAND, Santa Monica, 2022, p.89ss.

17 PAMMENT, J., Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, NATO Strategic Communications Centre of Excellence, Riga, 2022. Se resalta también la similitud de problemática de atribución respecto de los ciberataques. LIBICKI, Martin C., *Cyberdeterrence and Cyberwar*, RAND, Santa Mónica, 2009.

4.1. MARCO CONSTITUCIONAL

En el Derecho Constitucional, la CE1978 fue elaborada bajo un concepto clásico de Seguridad Interior, sin una alusión expresa al Ámbito Cognitivo (y con un legislador rodeado de un contexto tecnológico, de neurociencias y flujos de información abierta muy distante del actual). No obstante, la acción de protección cognitiva planteada actualmente es plenamente admisible dentro del marco constitucional. El Estado Social y Democrático de Derecho, en virtud de los artículos 8, 30, y 104 CE que proclaman los principios de seguridad, defensa y orden público y encomiendan su salvaguarda específicamente, junto a las Fuerzas Armadas (FAS)¹⁸, a las Fuerzas y Cuerpos de Seguridad del Estado (FyCSE).

Resulta evidente la extensión al Ámbito Cognitivo de la mencionada encomienda de protección propia del mandato constitucional, porque aquel es indisociable de las mentes de los ciudadanos, quienes están expuestos a las consecuencias negativas que puede tener sobre sus derechos y libertades la pérdida de confianza en las instituciones públicas y en la soberanía por causa de ataques cognitivos de desinformación. La protección de la estabilidad y libertad social, la capacidad de resiliencia y de seguridad cognitiva forma parte, por lo tanto, de los elementos de salvaguarda del orden público en perspectiva constitucional.

La Constitución Española, al encomendarles -además de a las Fuerzas Armadas- a las FyCSE la garantía de la soberanía e independencia de España, su integridad territorial y ordenamiento, confía también con ello la protección del Ámbito Cognitivo (que es parte de la integridad de los ciudadanos). Ello comporta la salvaguarda de las Libertades y Derechos Fundamentales en y desde el Ámbito Cognitivo: de un lado, “en” el Ámbito Cognitivo, porque atañe al conjunto de libertades y derechos de carácter fundamental que conllevan la libertad y derechos cognitivos; de otro, “desde” el Ámbito Cognitivo, porque se actúa desde los organismos de seguridad protegiendo dichas libertades y derechos al salvaguardar la estabilidad y el normal devenir e interacción de la ciudadanía con el Ámbito Cognitivo y los vectores y contenidos que confluyen en el mismo, evitando que estos últimos erosionen o conculquen los primeros. Con relación al grado de vigilancia sobre el Ámbito Cognitivo que correspondería a los organismos de Seguridad Interior, encontramos una clara analogía con el Ámbito Aeroespacial pues, en este, se requiere una cobertura permanente para garantizar la detección, interdicción y neutralización de vectores hostiles. Al mismo tiempo, se evidencian concomitancias con el Ámbito Ciberespacial a través del cual cursan, en buena parte (y con gran volumen de datos), las acciones cognitivas.

En cuanto a la limitación del llamado “derecho de acceso” a la información y de la transparencia administrativa -sobre la base del Secreto de Estado y de Seguridad

18 La problemática jurídica de la Defensa del Ámbito Cognitivo incorpora el concepto de Guerra Cognitiva. ESPONA, Rafael José de, “Las operaciones militares en el ámbito cognitivo: aspectos jurídicos” en: *Límites jurídicos de las operaciones actuales: nuevos desafíos*, Instituto Español de Estudios Estratégicos, Cuaderno de Estrategia nº 201, 2019, pp. 57-96. Por otra parte, el bloqueo de capacidades competenciales puede suscitarse por técnicas de *lawfare*: MANDELBLIT, Avihai, “*Lawfare: the Legal Front of the IDF*”, *Military and Strategic Affairs*, vol. 4, nº 1 (Abril 2012), pp. 51-57. TORRES SORIANO, Manuel R., “Los límites de la guerra de la información. Lecciones aprendidas tras los conflictos de Iraq y Afganistán”, *Revista Ejército*, nº 818, Junio 2009, pp. 14-22. WINGFIELD, Thomas C., “Legal Aspects of Offensive Information Operations in Space”, report, US Department of Defense, 2005.

Nacional- , ello es compatible con la salvaguarda de las Libertades y Derechos Fundamentales (como son la intimidad, la dignidad y la libertad de expresión). Por otra parte, en virtud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (basada en el GDPR UE 2018), la privacidad y protección de datos personales se ven reforzados.

En conjunto, el propio Estado de Derecho requiere una estabilidad cimentada en la confianza social sobre sus instituciones. La gestión de los Asuntos Públicos y la credibilidad de la información de carácter oficial e institucional necesitan encontrar un contexto de estabilidad y limpieza de ruido informativo o vectores de desinformación.

Además de las condiciones convencionales de protección del Ámbito Cognitivo, el marco constitucional admite la aplicación del denominado Derecho de Excepción, en contextos legales atípicos propios de las crisis, los Estados de Alarma, Excepción y Sitio (regulados por la Ley Orgánica. 4/1981 de 1 de junio) bajo los cuales es constitucionalmente válida cierta restricción temporal del ejercicio de Libertades y Derechos Fundamentales (a diferencia de la que acontece en el caso de la Situación de Interés para la Seguridad Nacional, regulada por la Ley 36/2015 de 28 de septiembre de Seguridad Nacional). Esta especialísima situación, además de su restricción normativa inherente a la singularidad que comporta, habría de aplicarse sobre el Ámbito Cognitivo con las debidas cautelas y garantías, sin limitar la libertad de expresión ni la autonomía de la opinión pública.

El precitado marco constitucional reviste al contexto institucional de organismos de Seguridad Interior e Inteligencia del adecuado respaldo jurídico institucional, el cual permitirá maximizar su acción de protección sobre el Ámbito Cognitivo.

4.2. MARCO COMPETENCIAL

Los organismos genéricamente competentes en materia de Seguridad Interior deben concordar su acción conforme a sus competencias administrativas específicas para incardinar adecuadamente su capacidad de acción sobre el Ámbito Cognitivo.

El contexto de Seguridad Nacional estructura el campo de la Seguridad Interior -junto con la Defensa y la Acción Exterior del Estado- para la debida protección de los ámbitos sobre los que se proyecta. La Ley de Seguridad Nacional 2015¹⁹ facilita las operaciones permanentes de monitorización y protección del Ámbito Cognitivo interno por cuanto que, aún no mencionándolo explícitamente (al igual que acontece con otros ámbitos, como el terrestre), se encuentra implícito, en tanto que los campos de especial interés para la Seguridad Nacional se definen en el art.10 *“aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos”* (entre los que, lógicamente, no puede obviarse el Ámbito Cognitivo), y establece un criterio de *numerus apertus*, al ser *“entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad*

19 Dicha ley (avalada por la STC 3-11-2016) introduce un marco normativo actual, propicio para la acción en el Ámbito Cognitivo, tanto en situación de normalidad como de crisis. Dicha disposición ha sido fruto de una orientación de estrategia de Estado que ha facilitado el desarrollo normativo e institucional del Sistema de Seguridad Nacional, otorga un marco normativo completo que no comporta en ningún caso la limitación de los derechos y libertades fundamentales de los ciudadanos, sino su salvaguarda.

marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente". El hecho de haber explicitado la ciberseguridad como una de las áreas concretas, incide en uno de los ámbitos de especial interacción con la acción cognitiva.

Siempre se garantizará la transparencia y conciencia social de la función institucional en materia de Seguridad Nacional -lo que incumbe a las operaciones en el Ámbito Cognitivo- en la medida en que se establezcan medidas de cultura de seguridad para el conocimiento y la sensibilización de la sociedad acerca de sus requerimientos, de los riesgos y amenazas susceptibles de comprometerla, así como del esfuerzo de los actores y órganos implicados en su salvaguarda, subrayando la conveniencia de informar -sin menoscabo de la debida seguridad de la información- sobre las *"medidas de anticipación, prevención, análisis, reacción, resistencia y recuperación respecto a dichos riesgos y amenazas"* (art. 5.2|2)

Los distintos documentos estratégicos de Seguridad Nacional reflejan lo expuesto en la práctica:

- La Estrategia de Seguridad Nacional 2017 (RD 1008/2017 de 1 de Diciembre) resalta la necesidad de contar con capacidades de monitorización y Alerta Temprana en gestión de crisis, pues *"es importante fomentar un enfoque preventivo y anticipatorio, para el que cobran particular relevancia el seguimiento permanente del entorno de seguridad y sus constantes cambios, los sistemas de inteligencia e información, el desarrollo de metodologías de análisis de riesgos y de instrumentos que contribuyan a la protección contra la desinformación"*. Sobre la resiliencia social y el mantenimiento de la estabilidad, se incide en que *"el fomento de la resiliencia de la sociedad y de las Administraciones adquiere una importancia esencial. Se trata de fortalecer la capacidad de recuperación ante posibles crisis, manteniendo la estabilidad necesaria para garantizar la continuidad en la acción del Gobierno dirigida a la protección de los ciudadanos y la provisión de los servicios esenciales, para retornar al estado de normalidad en el menor tiempo posible, de modo que se minimicen las consecuencias negativas sobre la seguridad y el bienestar de los ciudadanos"*.
- La Estrategia de Ciberseguridad Nacional 2019 (Orden PCI/487/2019, de 26 de abril), considera el ciberespacio como ámbito canalizador de la acción cognitiva y destaca la importancia de la preparación para la resiliencia cognitiva. Así, en su Introducción dispone que *"se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad"*.
- La Estrategia de Seguridad Nacional 2021 (RD 1150/2021, de 28 de diciembre) refiere explícitamente el Ámbito Cognitivo al afirmar que *"es un espacio más en el que ejercer influencia, que se suma a los tradicionales ámbitos físicos: terrestre, marítimo y aéreo. Los elementos que sí son inherentes a una campaña de desinformación son la voluntad de generar confusión y socavar la cohesión"*.

social; el uso coordinado de distintos medios para la creación y difusión de contenidos dirigidos a audiencias amplias; y la intención maliciosa con fines de desprestigio o influencia sobre el objetivo del ataque. Así, las campañas de desinformación suponen una grave amenaza para los procesos electorales. Por su potencial peligrosidad, cabe señalar las estrategias de desinformación de actores extranjeros, tanto estatales como no estatales, que desarrollan aparatos de propaganda con la intención de polarizar a la sociedad y minar su confianza en las instituciones”. Además de ello, señala los problemas de desinformación creciente, las injerencias digitales, el contexto de amenazas híbridas y la importancia de la lucha contra la desinformación. En este sentido, orienta la subsiguiente elaboración de una Estrategia Nacional de Lucha contra las Campañas de Desinformación (cuya precursora es la Orden P CM/1030/2020, de 30 de octubre, que aprueba el procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional).

Cabe añadir que, habida cuenta la confluencia en el Ámbito Cognitivo de vectores hostiles de distinto origen, la monitorización del mismo desde la perspectiva de la Seguridad Interior debe contemplar al tiempo la actividad que se desarrolla en la denominada “zona gris” (de los potenciales conflictos bélicos) la cual es susceptible de ser explotada por acciones cognitivas de posible origen militar externo, constitutivos de las denominadas Amenazas o Acciones Híbridas. Entre la Comunidad de Inteligencia, se desempeñan funciones de gran importancia para la protección del Ámbito Cognitivo, en perspectiva de defensa, acción policial y prospectiva de Estado.

4.3. LEGITIMACIÓN ÉTICA DE LA ACCIÓN INSTITUCIONAL

Considerando la especial sensibilidad del Ámbito Cognitivo y el gran alcance de sus efectos, se observa que estos son ampliamente proyectables desde las audiencias y *clusters* sociales a toda la población en su conjunto, pudiendo llegar a tener una gran repercusión sobre los factores de estabilidad y confianza social en las instituciones. Por lo tanto, la acción de los poderes públicos sobre el Ámbito Cognitivo (especialmente, desde los órganos del Sistema de Seguridad Nacional) debe no solo caracterizarse por su estricto cumplimiento normativo, sino por un alto grado de deontología funcional en el personal involucrado, respaldado por una sólida legitimación ética. Ello es así porque la acción sobre el Ámbito Cognitivo en perspectiva de Seguridad Interior (sea de vigilancia o de intervención) pone en un contexto complejo el mantenimiento del equilibrio del binomio seguridad+libertad que ha de respetarse en todo momento en el Estado Social y Democrático de Derecho, y con los principios éticos que lo iluminan, en un marco de aconfesionalidad y con especial sustento en la Declaración Universal de los Derechos Humanos.

La delimitación ética de la acción de protección de Seguridad Interior sobre el Ámbito Cognitivo -al igual que acontece en los demás ámbitos Físico y Cibernético- comporta un marco deontológico común que, en el caso específico de aquel, incide sobre aspectos especialmente relacionados con la capacidad de manipular las mentes sin apenas dejar rastro y poder actuar ocultamente, llegando incluso a generar efectos de alcance estratégico. Por lo tanto, se estima que el punto de partida de la limitación ética a la acción cognitiva de Seguridad Interior es la auto-restricción moral individual del personal funcional. En España, el componente ético a tener

en cuenta se encuentra en los principios del Estado de Derecho, la tradición jurídica y el acervo cultural español, los cuales son inherentes a la sociedad española e impregnan a los componentes de sus FyCSE.

Cabe una distinción sobre el grado de auto-restricción ética en la acción cognitiva por parte de los órganos de Seguridad Interior, dependiendo de si se trata de actividades de vigilancia o de intervención sobre el Ámbito Cognitivo.

Respecto de la acción de vigilancia, en tanto que la salvaguarda de las Libertades y Derechos Fundamentales requiere la garantía de una protección cognitiva efectiva que no puede iniciarse sin un conocimiento pleno del escenario, la legitimación ética de la vigilancia del Ámbito Cognitivo permite actividades como el análisis del entorno de la información (que, en todo caso, contemplará datos personales de manera agregada y anónima) y la monitorización de su dinámica (conformada por vectores cognitivos y modulaciones de contenidos), los parámetros, premisas epistemológicas y esquemas mentales de la población, su eventual génesis inducida por agentes de influencia (orientada a la Opinión Pública o a otras corrientes de pensamiento, percepción, actitud o emoción asociadas a *clusters* sociales) y sus condiciones de estabilidad, desenvoltura y resiliencia.

En cuanto a la acción de intervención, la limitación es mucho mayor que la anterior, por cuanto que es imprescindible que toda acción incisiva sobre el Ámbito Cognitivo esté estrictamente orientada a la protección sin limitación de libertades y sin influir en los contenidos y vectores cognitivos. Es éticamente aceptable la intervención anticipativa al delito, el apoyo a la estabilización (i.e. modulando la energía social), y la evitación de condiciones propicias para una explotación invasiva de vectores hostiles, de injerencia o desestabilizadores. Ello no menoscaba el libre albedrío social, sino que facilita su normal devenir.

5. LA ACCIÓN DE SEGURIDAD INTERIOR SOBRE EL ÁMBITO COGNITIVO

La acción de las instituciones competentes en materia de Seguridad Interior (FyCSE y otras) en el Ámbito Cognitivo en general, tiene como finalidad primera protegerlo, gestionando el mantenimiento del Orden Público en dicha dimensión, y garantizar las Libertades y Derechos Fundamentales de la población, evitando que sufra daño cognitivo. En último término, es su fin el mantenimiento de la estabilidad y la contribución a la resiliencia social.

La participación de las FyCSE en acciones concurrentes con actividades cognitivas de los poderes del Estado (como la difusión de información oficial pública en materia de prevención de riesgos o protección civil) puede obstaculizarse debido a la heterogeneidad conceptual y jurídica relativa a la actividad en el Ámbito Cognitivo respecto de otros órganos estatales (generándose una discordancia operativa inter-institucional, de manera que la eficacia de la acción se puede resentir). Por consiguiente, es preciso que la doctrina elaborada para la acción institucional sobre el Ámbito Cognitivo sirva adecuadamente a los poderes constitucionales para una verdadera acción integrada, además de aquella específica de cada organismo. El objeto de la acción debe ser común, si bien abordado desde las competencias y con las capacidades operativas propias de cada organismo público.

Si el objeto de la acción sobre el Ámbito Cognitivo en general es sencillo de definir, más complejo resulta determinar singularmente elementos del mismo (tales como Centros de Gravedad, vectores o narrativas concretos). Asimismo, el objeto de la acción se desdobra en dos variantes, que son la acción de vigilancia y la de intervención. Si, en el primer caso, la actividad es de mera observación (detallada y estructurada), en el segundo se trata de actuar sobre el Ámbito Cognitivo para modificar, aunque sea mínimamente, su composición. Todo ello conlleva la necesidad de disponer de los adecuados protocolos procedimentales para una acción que será descriptiva, predictiva, preventiva, proactiva o reactiva, dependiendo del caso concreto de aplicación.

Respecto de la acción de vigilancia, la mera observación no supone propiamente actuar sobre el Ámbito Cognitivo, y comporta actividades del tipo descriptivo y predictivo. El actor responsable de estas tareas es de índole pasivo, sin intervenir sobre los parámetros y contenidos de dicho ámbito. Respecto de la acción de intervención, en tanto que la protección cognitiva efectiva no puede iniciarse sin un conocimiento pleno del escenario, el rastreo (“patrullaje cognitivo”) y monitorización del Ámbito Cognitivo permite actividades como el análisis del entorno de la información (que solo de manera agregada y anónima podrá procesar datos personales) y la monitorización de su dinámica (conformada por vectores cognitivos y contenidos modulados), los parámetros, premisas analíticas y esquemas mentales de la población, su eventual génesis inducida (por agentes de influencia orientada a la Opinión Pública o a otras corrientes de pensamiento, percepción, actitud o emoción asociadas a *clusters* sociales, incluyendo las malinterpretaciones inducidas entre las que se incluye el denominado *conspiracionismo* objeto de estudio por el CCN-CERT desde el Observatorio Digital ELISA²⁰) y sus condiciones de estabilidad, desenvoltura y resiliencia. La acción de intervención del Ámbito Cognitivo comporta los siguientes cometidos desglosados: monitorización y rastreo, detección y evidenciación, predicción, Alerta Temprana y seguimiento.

La acción de intervención sobre el Ámbito Cognitivo supone entrar en él de manera activa para influir de alguna manera sobre y, en su caso, desde el mismo. Esta actuación, a su vez, puede ser de tipo preventivo, proactivo o reactivo, según se materialice antes o después de la producción de un vector o injerencia, influencia perniciosa o desestabilización cognitiva que se pretende confrontar con carácter disuasorio, corrector, neutralizador o destructor, de manera o indirecta.

A diferencia de la acción de vigilancia que, por definición, ha de ser permanente y con capacidad de maximizar su alcance para cubrir en lo posible el gran espectro del

20 KAVANAGH, Jennifer, RICH, Michael D., *Truth Decay. An Initial Exploration of the Disminishing Role of Facts and Analysis in American Public Life*, RAND, Santa Mónica, 2018, pp.191-206. CCN-CERT, *Observatorio Digital ELISA – Laboratorio para el análisis de la Desinformación (Antiglobalismo)*, CCN-CERT, Septiembre 2020. Con posterioridad al informe ELISA, han proliferado nuevas manifestaciones del citado fenómeno, de manera aislada o concatenada; HERAKLIO, Pablo, “La Guerra Cognitiva Mundial afecta a las Sociedades Globalizadas y provoca situaciones S.A.D. I/III”, Publicado el 15 de noviembre de 2021 / Disponible en: <https://kaosenlared.net/la-guerra-cognitiva-mundial-afecta-a-las-sociedades-globalizadas-y-provoca-situaciones-s-a-d-i-iii/> - Consultado: 18-8-2022. ROCKEFELLER FOUNDATION & GBN, Scenarios for the Future of Technology and International Development, Report RF & GBN, May 2010. SILBERGLITT, Richard, ANTON, Philip S., HOWELL, David R., WONG, Anny, GASSMAN, Natalie, JACKSON, Brian A., LANDREE, Eric, PFLEEGER, Shari Lawrence, NEWTON, Elaine M., WU, Felicia, *The Global Technology Revolution 2020, In-Depth Analyses. Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, RAND, Santa Monica, 2006, p. xix. OSTERHOLM, Michael T., “Preparing for the Next Pandemic”, *Foreign Affairs*, Vol.84, nº 4, July/August 2005, pp.24-37.

Ámbito Cognitivo, la acción de intervención constituye un recurso para las FyCSE de empleo más restrictivo, tanto en su alcance como en la ocasionalidad temporal.

Se consideran como criterios básicos operativos (que complementan los de carácter normativos y ético) de utilización de las acciones de intervención sobre el Ámbito Cognitivo, que se aplican asimismo para su configuración intrínseca, los de oportunidad, proporcionalidad, limitación de alcance, pre-definición y delimitación de efectos.

6. CONSIDERACIONES SOBRE METODOLOGÍA Y STRATCOM

Las técnicas de acción sobre el Ámbito Cognitivo requieren una metodología adecuada. Primeramente, es necesario conocer los parámetros concretos del mismo, partiendo de la concreción de los Centros de Gravedad, del análisis y ponderación de la Energía Social y de la evaluación de la intensidad y arraigo de vectores cognitivos. En los aspectos de vigilancia, se requiere analizar indicadores y señales, diseñar procedimientos para protocolos predictivos, preventivos, proactivos y reactivos, de rastreo y de Alerta Temprana, así como un planeamiento tanto de operaciones permanentes como ocasionales. En la intervención, es necesaria la coordinación de concordancias de las acciones paralelas en los Ámbitos Físico y Cibernético, con un determinado diseño de contra-narrativas y mediante el empleo de la Comunicación Estratégica (STRATCOM) en tanto que herramienta funcional avanzada que integra capacidades de inteligencia y acción psicológica²¹. La armonización metodológica es fundamental en lo que atañe a la cooperación público-privada.

Partiendo de una adecuada parametrización del Ámbito Cognitivo, la vigilancia adecuada sobre el Ámbito Cognitivo comporta una operación permanente (la cual, en todo caso, podría ser ocasionalmente reforzada *ad-hoc* ante determinadas contingencias) combinando técnicas de obtención y elaboración automatizadas²² -especialmente eficaz respecto de la interacción de aquel con el Ámbito Cibernético- junto con funciones HUMINT respecto del Ámbito Físico. Respecto del caudal cognitivo presente en el Ciberespacio, para que el resultado de la captación y procesamiento de la ingente cantidad de *BigData* sea útil, habrá de ser enriquecido cualitativamente con los denominados *MicroData*, para su tratamiento mediante procesos de Inteligencia Artificial de apoyo a partir de algoritmos (cuyo componente ético también atañe a su diseño y aplicación). La integración de todos los procesos de elaboración confluye en un análisis de meta-inteligencia.

La Ingeniería Social Inversa (no opuesta) es una de las metodologías de mayor utilidad para evidenciar las intervenciones complejas en el Ámbito Cognitivo. Emplea

21 SÁNCHEZ BENITEZ, Sergio, "La comunicación estratégica como política pública", Documento de Opinión nº 21/2011, IEEE-CESEDEN, 2011. SILVELA DÍAZ-CRIADO, Enrique, en: Diego Mazón Born (coord.), *La Comunicación Estratégica*, "Comunicación estratégica: origen y evolución del concepto", Documento de Seguridad y Defensa nº 72, IEEE-CESEDEN, 2017, pp. 13-34. VV.AA., "Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response and Recovery", Final Report RAND, 2008, p. 20. NATO STRATCOM CoE, "Hybrid Threats. A Strategic Communications Perspective", NATO Strategic Communications Centre of Excellence, Riga, 2019, pp. 12, 13 y 20. EMAD, *Publicación Doctrinal Conjunta PDC-10. Doctrina de Comunicación Estratégica*, Estado Mayor de la Defensa, 2021.

22 NATO STRATCOM CoE, *Social Media Monitoring Tools: An In-Depth Look.*, NATO Strategic Communications Centre of Excellence, Riga, 2022.

una técnica analítica deductiva que consiste en inferir la eventual acción de Ingeniería Social presente, partiendo del análisis de efectos y parámetros sociales. La Ingeniería Social inversa es, en su mayor parte, aplicada sobre el Ámbito Cognitivo.

La actuación de intervención sobre el Ámbito Cognitivo puede ser requerida para su debida protección o estabilización, antes, durante o después de un impacto negativo en términos de Seguridad Cognitiva, de forma preventiva, proactiva o reactiva. Es también preciso tener en cuenta acciones no cognitivas que confluyen en las operaciones de protección sobre el Ámbito Cognitivo.

Como técnica avanzada de intervención sobre el Ámbito Cognitivo, la metodología STRATCOM, se conceptúa como la integración de todas las capacidades de comunicación, técnicas de gestión de la información -funciones y actividades de Asuntos Públicos, Acción Psicológica, Inteligencia y Contrainteligencia- con otras actividades sobre el Ámbito Cognitivo, para maximizar la capacidad de influencia cognitiva y modelar el entorno de la información, con alcance estratégico.

La cooperación público-privada es imprescindible para una adecuada protección del Ámbito Cognitivo. La participación activa del sector privado, respecto del apoyo e interacción en el Ámbito Cognitivo, dentro del Sistema de Seguridad Nacional en general y con las FyCSE en particular, es una tendencia creciente -especialmente en el entorno OCDE, UE y OTAN- de gran utilidad para la actividad de protección en el Ámbito Cognitivo. La contribución privada a la Seguridad Cognitiva es fundamental para la acción de vigilancia y puede ser muy relevante en determinadas acciones de intervención. En este último sentido, constituye un recurso susceptible de integrarse en las metodologías STRATCOM, permitiendo reforzar los mecanismos de Comunicación Estratégica del Estado, contando con un mapa de recursos comunicativos susceptibles de ser empleados a nivel estratégico y en operaciones de protección del Ámbito Cognitivo.

7. CONCLUSIONES

Siendo el propósito del presente estudio contribuir a dotar de una adecuada capacidad funcional a los organismos competentes en materia de Seguridad Interior para la oportuna vigilancia y, en su caso, intervención sobre el Ámbito Cognitivo, se recapitula lo tratado en base a las conclusiones que se exponen a continuación:

- La protección del Ámbito Cognitivo, en tanto que dimensión de aplicación de la Seguridad Nacional, requiere la acción específica de Seguridad Interior.
- Las potenciales misiones de los organismos de seguridad del Estado sobre el Ámbito Cognitivo, con pleno engarce en el marco de la CE1978, han de configurarse de acuerdo con la acotación y estructuración de dicho ámbito, siendo dotadas de una actualización y desarrollo normativo y regulación institucional acordes con ello.
- Se necesita una doctrina propia adaptada y dotada de una línea de acción permanente de mejora continua, con una visión holística e integrada, acompañada de la adquisición de nuevas capacidades y medios tecnológicos apropiados.
- Para una adecuada metodología de acción, es imprescindible conocer el estado del arte de las neurociencias y TICs en tanto que permiten desarrollar los

medios de acción propio e inferir las acciones hostiles, criminales, terroristas o bélicas híbridas.

- Además de los riesgos y amenazas propios de la acción hostil militar, terrorista o criminal sobre el Ámbito Cognitivo, se plantea el riesgo de desconfianza y desestabilización sistémica por parte de la población respecto de la acción cognitiva de FyCSE, lo cual habrá de ser evitado mediante una adecuada política de transparencia de la función pública.
- La cooperación público-privada es especialmente relevante al respecto de la acción de protección sobre el Ámbito Cognitivo, lo cual también contribuirá al tiempo a la confianza de los agentes sociales y de la población.

En definitiva, se trata de garantizar la adecuada protección del Ámbito Cognitivo salvaguardando las libertades y derechos fundamentales para la Seguridad de España.

BIBLIOGRAFÍA

ARONHIME, Lawrence Aronhime, COCRON, Alexander (sup.), *Countering cognitive warfare: awareness and resilience*, Johns Hopkins University & Imperial College London, 20 May 2021.

AVERY, Thomas, "Popper on "Social Engineering": A Classical Liberal View", *Reason Papers*, vol. 26 (2000) pp.29-38.

CCN-CERT, *Desinformación en el ciberespacio*, CCN-CERT / BP 13, Febrero 2019.

CCN-CERT, *Observatorio Digital ELISA – Laboratorio para el análisis de la Desinformación (Antiglobalismo)*, CCN-CERT, Septiembre 2020.

DSN, Estrategia de Seguridad Nacional 2021, Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

EMAD, Publicación Doctrinal Conjunta PDC-01 (A) *Doctrina para el empleo de las FAS*, Estado Mayor de la Defensa, 2018.

EMAD, Publicación Doctrinal Conjunta PDC-10. *Doctrina de Comunicación Estratégica*, Estado Mayor de la Defensa, 2021.

ESPONA, Rafael José de, "Las operaciones militares en el ámbito cognitivo: aspectos jurídicos" en: *Límites jurídicos de las operaciones actuales: nuevos desafíos*, Instituto Español de Estudios Estratégicos, Cuaderno de Estrategia nº 201, 2019, pp. 57-96.

ESPONA, Rafael José de, "Seguridad energética y guerra psicológica", Instituto Español de Estudios Estratégicos (en línea), Documento de Opinión 66/2016, 1 de Julio de 2016.

GONZÁLEZ, Wenceslao. J., "Tipos de diseño, innovaciones democráticas y relaciones internacionales", en ESTANY, A. y GENSOLLEN, M. (eds), *Diseño institucional e innovaciones democráticas*, Eximia-Universidad Autónoma de Barcelona-Universidad Autónoma de Aguascalientes, Barcelona, en prensa.

GONZALEZ, Wenceslao. J., "From Intelligence to Rationality of Minds and Machines in Contemporary Society: The Sciences of Design and the Role of Information", *Minds*

and Machines, v. 27, n. 3, (2017), pp. 397-424. DOI: 10.1007/s11023-017-9439-0. Disponible en <https://link.springer.com/article/10.1007/s11023-017-9439-0>

GONZÁLEZ, Wenceslao. J., "Internet en su vertiente científica: Predicción y prescripción ante la complejidad", *Artefactos: Revista de Estudios de la Ciencia y la Tecnología*, v. 7, n. 2, (2018), 2ª época, pp. 75-97. DOI: <http://dx.doi.org/10.14201/art2018717597>.

GONZÁLEZ, Wenceslao. J., "Complejidad dinámica en Internet como plataforma de información y comunicación: Análisis filosófico desde la perspectiva de Ciencias de Diseño y el papel de la predicción", *Informação e Sociedade: Estudos*, v. 28, n. 1, (2018), pp. 155-168.

GONZÁLEZ, Wenceslao. J., "Internet y Economía: Análisis de una relación multivariada en el contexto de la complejidad", *Energeia: Revista internacional de Filosofía y Epistemología de las Ciencias Económicas*, v. 6, n. 6, (2019), pp. 11-36. Disponible en: https://abfcfc9a-c7ef-4730-b66e-0a415ef434c0.filesusr.com/ugd/e46a96_b400a-f5a739e4310a31b7e952244745d.pdf

GONZALEZ, Wenceslao. J., "La dimensión social de Internet: Análisis filosófico-metodológico desde la complejidad", *Artefactos: Revista de Estudios de la Ciencia y la Tecnología*, v. 9, n. 1, (2020), 2ª época, pp. 101-129. DOI: <http://dx.doi.org/10.14201/art2020101129>. Disponible en: <https://revistas.usal.es/index.php/artefactos/article/view/art2020101129>.

GONZÁLEZ, Wenceslao. J., "Electronic Economy, Internet and Business Legitimacy", en RENDTORFF, J. D. (ed), *Handbook of Business Legitimacy: Responsibility, Ethics and Society*, Springer, Dordrecht, 2020, pp. 1-19 (printed version, pp. 1327-1347). DOI: https://doi.org/10.1007/978-3-319-68845-9_84-1.

GONZALEZ, Wenceslao. J. (ed), *Language and Scientific Research*, Palgrave Macmillan, Cham, 2021. Disponible en: <https://www.springer.com/in/book/978-3-030-60536-0>.

JUSLIN, Patrik, VASTFJALL, Daniel, "Emotional responses to music: The need to consider underlying mechanisms", *Behavioral and Brain Sciences*, n.º 31, 2008, pp. 559-621.

KAVANAGH, Jennifer, RICH, Michael D., *Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, RAND, Santa Mónica, 2018, pp.191-206.

KRISHNAN, Armin, "From Psyops to Neurowar: What are the Dangers?", ISAC-ISSS Conference, Austin, November 2014.

LEE, Mary Lee, BOUDREAUX, Benjamin, CHATURVEDI, Ritika, ROMANOSKY, Sasha, DOWING, Bryce, *The Internet of Bodies. Opportunities, Risks, and Governance*, RAND, Santa Monica, 2020, pp.23ss.

LEWIS, James A., "Cognitive Effect and State Conflict in Cyberspace", CSIS, 2018.

LIBICKI, Martin C., *Cyberdeterrence and Cyberwar*, RAND, Santa Mónica, 2009.

LOVEGROVE, Kitty, "The acoustic world on influence: how Musicology illuminates Strategic Communications", *Defence Strategic Communications*, vol. 5, Otoño 2018, pp. 13-49.

MANDELBLIT, Avihai, "Lawfare: the Legal Front of the IDF", *Military and Strategic Affairs*, vol. 4, n.º 1 (Abril 2012), pp. 51-57.

MOUTON, Francois, PILLAY, K., VAN`T WOUT, M.C., "The Technological Evolution of Psychological Operations Throughout History", en: Clarke, N.I., Furnell S.M. (editors), *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2016 Frankfurt), ed. Plymouth University, Plymouth, 2016, pp.266-278.

NATO STRATCOM CoE, "Hybrid Threats. A Strategic Communications Perspective", NATO Strategic Communications Centre of Excellence, Riga, 2019, pp. 12, 13 y 20.

NATO STRATCOM CoE-SINGULAREX, "The Black Market for Social Media Manipulation", NATO Strategic Communications Centre of Excellence, Riga, 2018.

NATO STRATCOM CoE, *Social Media Monitoring Tools: An In-Depth Look.*, NATO Strategic Communications Centre of Excellence, Riga, 2022.

PAMMENT, J., Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, NATO Strategic Communications Centre of Excellence, Riga, 2022.

SÁNCHEZ BENITEZ, Sergio, "La comunicación estratégica como política pública", Documento de Opinión nº 21/2011, IEEE-CESEDEN, 2011.

SIBONI, Gabi, "The First Cognitive War", en: Kurz, A., Brom, S (eds.), *Strategic Survey for Israel 2016-2017*, Institute for National Security Studies, Tel Aviv, 2016.

SILBERGLITT, Richard, ANTON, Philip S., HOWELL, David R., WONG, Anny, GASSMAN, Natalie, JACKSON, Brian A., LANDREE, Eric, PFLEEGER, Shari Lawrence, NEWTON, Elaine M. , WU, Felicia, *The Global Technology Revolution 2020, In-Depth Analyses. Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, RAND, Santa Monica, 2006, p. xix.

SILVELA DÍAZ-CRIADO, Enrique, en: Diego Mazón Born (coord.), *La Comunicación Estratégica*, "Comunicación estratégica: origen y evolución del concepto", Documento de Seguridad y Defensa nº 72, IEEE-CESEDEN, 2017, pp. 13-34.

TORRES SORIANO, Manuel R., "Los límites de la guerra de la información. Lecciones aprendidas tras los conflictos de Iraq y Afganistán", *Revista Ejército*, nº 818, Junio 2009, pp. 14-22.

U.S. ARMY, *From PSYOP to MindWar: The Psychology of Victory by Colonel Paul E. Valley, Commander, with Major Michael A. Aquino, PSYOP Research & Analysis Team Leader*, Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, CA, 1980.

VV.AA., "Analysis of Risk Communication Strategies and Approaches with At-Risk Populations to Enhance Emergency Preparedness, Response and Recovery", Final Report RAND, 2008, p. 20.

VV.AA., *Rivalry in the Information Sphere. Russian Conceptions of Information Confrontation*, RAND, Santa Monica, 2022, p.89ss.

WINGFIELD, Thomas C., "Legal Aspects of Offensive Information Operations in Space", report, US Department of Defense, 2005.

