

TECNOLOGÍAS UTILIZADAS EN SERVICIOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

Vanessa DÍAZ*

SUMARIO: I. *Introducción*. II. *Clasificación de tecnologías y sistemas de inteligencia*. III. *Otras fuentes de información en servicios de inteligencia y contrainteligencia*. IV. *Diversas tecnologías utilizadas para actividades de seguridad nacional*. V. *Sociedad proactiva en actividades de video-vigilancia*. VI. *Conclusiones*. VII. *Bibliohemerografía*.

I. INTRODUCCIÓN

La proliferación de tecnologías utilizadas en actividades de inteligencia y contrainteligencia ha tenido dos etapas, básicamente: durante la Guerra Fría y tras los ataques terroristas del 11 de septiembre de 2001. En la Guerra Fría se vivió una de las carreras armamentistas más importantes en la historia de la humanidad; sin embargo, el desarrollo tecnológico de las últimas décadas ha permitido un avance significativo en áreas de inteligencia y contrainteligencia.

Por cuestiones metodológicas debemos establecer el marco referencial de servicios de inteligencia, el cual, para fines de esta investigación, se entiende como toda actividad que proporciona al gobierno información útil a través de la recolección, procesamiento y análisis de la información. Las actividades de inteligencia se dividen en estratégica y operacional o táctica. A su vez, la inteligencia se clasifica por sectores: exterior, interior, militar, criminal, económica, tecnológica, empresarial, etcétera.¹

* Candidata a doctora en derecho por la Universidad de Tasmania; académica en el Instituto de Investigaciones Jurídicas de la UNAM (diazd@postoffice.utas.edu.au).

¹ *Cfr.* Johnson, Loch K., “Ethical Intelligence: A Contradiction in Terms?”, *Intelligence and National Security*, 24 de junio de 2009, pp. 367 y 368; Johnson, Loch K., “Preface to a Theory of Strategic Intelligence”, *International Journal of Intelligence and Counterintelligence*, núm. 16, invierno de 2003-2004, pp. 638-663.

En este trabajo se desarrollan —de manera enunciativa, mas no limitativa— algunas tecnologías utilizadas en actividades de inteligencia y contrainteligencia. La investigación se centra en la clasificación de productos y tecnologías utilizados en actividades de inteligencia y de defensa a partir de los trabajos de Johnson,² Haggerty,³ Clancey⁴ y Lyon.⁵ Además, se incluyen tecnologías químicas, biológicas, geofísicas y biométricas, por considerarlas relevantes en la discusión de este estudio.

Cabe señalar que no son objeto de estudio las medidas de control armamentista ni de desarme implementadas por diversas organizaciones internacionales; sin embargo, por cuestiones metodológicas, en los apartados sobre tecnología química, biológica y geofísica se mencionan los convenios relativos a la prohibición, destrucción y almacenamiento de armas de destrucción masiva (ADM). Ahora bien, en relación con la tecnología biométrica, se resalta la omisión de convenios o tratados internacionales relativos a la implementación de este tipo de tecnología.

En este mismo sentido, es importante resaltar las recientes actividades de vigilancia llevadas a cabo por la sociedad civil de una manera proactiva. Esta situación es una fase importante dentro del reposicionamiento del ciudadano como presupuesto básico de cualquier democracia. Sin embargo, debe reconocerse que el factor tecnológico ha impulsado este reposicionamiento.

El trabajo está dividido en cinco secciones. La primera sección (II) se identifica con la clasificación de tecnologías y los sistemas de información utilizados en las diferentes etapas de los servicios de inteligencia y contrainteligencia. La segunda sección (III) versa sobre otras fuentes de información implementadas. Mientras que en la tercera (IV) se identifican las diferentes tecnologías utilizadas para cuestiones de seguridad nacional. En la cuarta (V) se abordan versa sobre los diferentes proyectos desarrollados para

² Johnson, Loch K. (ed.), *The Oxford Handbook of National Security Intelligence*, Oxford University Press, 2010, 886 pp.; Johnson, Loch K. y Wirtz, James, *Intelligence and National Security: The Secret World of Spies-An Anthology*, 2a. ed., Oxford University Press, 2007, 564 pp.; Johnson, Loch K., *National Security Intelligence: Secret Operations in Defense of the Democracies*, Cambridge, Polity, 2012; Johnson, Loch K., *Bombs, Bugs, and Thugs: Intelligence and America's Quest for Security*, New York University Press, 2002, 298 pp.

³ Haggerty, Kevin D. y Ericson, Richard V. (eds.), *The New Politics of Surveillance and Visibility*, Canadá, University of Toronto Press, 2006, pp. 386.

⁴ Clancey, Garner y Lulham, Rohan, "Natural Surveillance", conferencia presentada en The Surveillance in/and Everyday Life Conference, Australia, Universidad de Sydney, 20-21 de febrero de 2012.

⁵ Lyon, David, "Surveillance after September 11 2001", *Sociological Research Online*, núm. 6, vol. 3, 2001.

una sociedad proactiva en actividades de video-vigilancia. Finalmente, en la quinta sección (VI) se brindan las conclusiones.

II. CLASIFICACIÓN DE TECNOLOGÍAS Y SISTEMAS DE INTELIGENCIA

Existen diversas tecnologías y sistemas de inteligencia utilizados en las distintas etapas de los servicios de inteligencia, los cuales pueden clasificarse en un núcleo básico, planificación, recolección, procesamiento, incluido el análisis, difusión y seguridad:⁶

- 1) En el núcleo básico se comprende la arquitectura y diseño de los sistemas, su interoperabilidad y compatibilidad; generalmente está compuesto por software y hardware, que constituyen las plataformas tecnológicas para productos de cifrado o encriptado.

Aquí se puede destacar la función, por ejemplo, de las siguientes agencias: la estadounidense *National Security Agency* (NSA),⁷ la británica *Government Communication Headquarters* (GCHQ),⁸ la española Centro Criptológico Nacional (CCN),⁹ y la australiana *Defence Signals Directorate* (DSD).¹⁰

Para la Oficina Federal alemana para la Seguridad de la Información (BSI, por sus acrónimos en alemán), la empresa Secunet desarrolló el núcleo básico —la arquitectura de red— que permite el procesamiento, almacenamiento y transmisión de documentos clasificados, así como de otros datos sensibles de manera segura. El producto es conocido como SINA, y cuenta con la aprobación para su procesamiento y transmisión de documentos clasificados de la OTAN y de la Unión Europea.¹¹

- 2) En la planificación se utilizan sistemas para dirigir y priorizar las tareas o necesidades, tanto para los usuarios como para los destinatarios.

⁶ Johnson, Loch K., *Bombs, Bugs, and Thugs: Intelligence and America's Quest for Security*, cit., p. 298.

⁷ Véase <http://www.nsa.gov/index.shtml> (consultada el 9 de agosto de 2013).

⁸ Véase <http://www.gchq.gov.uk/Pages/homepage.aspx> (consultada el 9 de agosto de 2013).

⁹ Véase <https://www.ccn.cni.es/> (consultada el 9 de agosto de 2013).

¹⁰ Véase <http://www.dsd.gov.au/index.htm> (consultada el 9 de agosto de 2013).

¹¹ Para mayor información sobre SINA puede verse el portal oficial de la empresa Secunet: <http://www.secunet.com/en/products-services/high-security/sina/> (consultada el 10 de agosto de 2013). La traducción es nuestra.

Un claro ejemplo es el Sistema Informático de Coordinación de Operaciones Antiterroristas (SICOA) de España. El SICOA es un programa y base de datos que sigue “de forma permanente” las investigaciones de la policía, la guardia civil y el Centro Nacional de Inteligencia, para evitar duplicidades y establecer caminos de coordinación en las operaciones antiterroristas.

En este mismo sentido, encontramos el Sistema Único de Información Criminal (SUIC) de México. El SUIC concentra y correlaciona diversas bases de datos que tiene el Estado en sus distintos órdenes de gobierno con el objetivo de coordinar las investigaciones criminales, especialmente en la lucha contra el narcotráfico.

Los sistemas de recolección son múltiples y variados, operan diversas plataformas.

Este tipo de sistemas se basa en redes de comunicación:

- Comunicaciones tradicionales: teléfono móvil y fijo, radio, transmisores, Internet, etcétera.
- Detección de la presencia de objetos o superficies y ubicación de su posición exacta, movimiento a distancia y acústica en algunos casos: radares, sistemas de posicionamiento global —GPS, GMS, GPRS—, etcétera.

Pero se complementa con la información proporcionada y recolectada por imágenes a través de cámaras o videocámaras, satélites y aviones no tripulados —conocidos como *Drones*—.

También se incluyen los sistemas electro-ópticos, los cuales abarcan láseres en la longitud de onda azul-verde —capaz de traspasar el agua, para las comunicaciones entre satélites y submarinos—, cables de fibra óptica e infrarrojos; estos últimos son utilizados para detectar camuflajes.

La empresa Getac¹² ofrece software especialmente para fotografías con aplicaciones de GPS. Mientras que la empresa AOPTIX Technologies colaboró con la fuerza aérea norteamericana para perfeccionar el programa Air-Ground Lasercom System.¹³ Por su parte, la

¹² Véase http://en.getac.com/products/Getac-Camera/Getac-Camera_overview.html (consultada el 16 de agosto de 2013).

¹³ Para conocer más del proyecto consúltese el portal oficial de la empresa AOPTIX Technologies: <http://www.aoptix.com/news-events/press-releases/71-defense-lasercom-news-air-force-flight-test-complete> (consultada el 16 de agosto de 2013).

empresa Thales provee a la fuerza armada francesa productos para el sistema global de navegación por satélite (GNSS).¹⁴

- 3) Para el procesamiento y análisis se utilizan sistemas que reciben, convierten e interrelacionan los datos, efectuando un análisis de los mismos.

Uno de los sistemas más completos de recolección de información es el denominado proyecto ECHELON;¹⁵ sistema mundial de interceptación de comunicaciones (COMINT) creado por los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda para vigilar rutinariamente y de manera indiscriminada, y registrar todas las formas de comunicaciones electrónicas en todo el mundo (tanto militares como civiles), supervisado por la *National Security Agency* (NSA).

Las agencias de estos países seleccionan la información que les sea útil a través de dos sistemas: el sistema de inteligencia artificial, llamado Memex, que utiliza palabras clave,¹⁶ y el programa de reconocimiento automático de voz, llamado Oratory, para interceptar llamadas telefónicas.

La *National Security Agency* (NSA) desarrolló dos programas para mejorar las capacidades de ECHELON. Uno de estos programas es *Oasis*, el cual crea automáticamente, legibles por máquina, transcripciones de emisiones de televisión y de audio; puede distinguir los ponentes individuales y detectar las características personales (como género). El otro programa es *Fluent*, el cual permite búsquedas de palabras clave de los materiales que no están en inglés. Esta herramienta no sólo busca los documentos pertinentes, sino que también los traduce, aunque el número de lenguas que actualmente se pueden traducir, al parecer, es limitado (en ruso, chino, portugués, serbo-croata, coreano y ucraniano). Además, *Fluent* muestra la frecuencia con la que se utiliza una palabra dada en un documento y puede manejar alternos deletreos en un plazo de búsqueda.

Actualmente existen algunas versiones muy similares de ECHELON: el español “Programa Santiago”, administrado por el Ministe-

¹⁴ Para mayor información véase el portal oficial de la empresa Thales: http://www.thalesgroup.com/Press_Releases/Markets/Aerospace/2012/20120405_Thales_to_provide_GPS_SA_ASM_receivers_for_French_Navy_Lynx_helicopters/ (consultada el 16 de agosto de 2013).

¹⁵ Véase <http://actionamerica.org/echelon/echelonwhat.html> (consultada el 16 de agosto de 2013).

¹⁶ Véase <http://www.memex.com/news/memex-implements-michigan-criminal-intelligence-system> (consultada el 16 de agosto de 2013).

rio de Defensa, cuyo objetivo principal es la captación de emisiones electromagnéticas y de imágenes en las zonas definidas como de interés estratégico para la seguridad nacional española.

En este sentido, cabe señalar que la empresa WCC Smart Search and Match¹⁷ desarrolló un sistema de información denominado ELISE, cuyos motores de búsqueda conjuntan información personal e información biométrica de individuos. Dicho sistema es utilizado para control migratorio e investigaciones criminales.

- 4) Por lo que respecta a los sistemas y tecnologías de difusión, éstos se encargan de canalizar la información a los usuarios finales; son programas o redes de comunicación entre servicios de información, generalmente de centros nacionales de inteligencia a los órganos de decisión —presidencia o primer ministro—.
- 5) Por último, los sistemas y tecnologías de seguridad son aquellos destinados a proteger los vínculos, depósitos y redes por donde transita la información, así como controlar su acceso. Programas de cifrado sobre datos, voz, sistemas de protección frente a intrusiones.

III. OTRAS FUENTES DE INFORMACIÓN EN SERVICIOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

En esta sección se hace mención de algunos de los diferentes sistemas de información y agentes que también son implementados en los servicios de inteligencia y contrainteligencia con el objetivo de recolectar información.

1. *Sistemas de información*

Total Information Awareness (TIA) es un proyecto del Departamento de Defensa estadounidense. TIA está diseñado para recopilar datos personales a gran escala, incluyendo correos electrónicos, llamadas telefónicas, registros financieros, hábitos de transporte, información clínica, entre otros. Incluye el software para predecir el comportamiento de un individuo sobre la base de lo que esa persona hace en línea.

Carnivore Diagnostic Tool (DCS 1000).¹⁸ *Carnivore* es un sistema del FBI que es utilizado para la lucha contra el terrorismo, el espionaje, la guerra de

¹⁷ Para mayor información sobre ELISE véase el portal oficial de la empresa WCC Smart Search & Match: http://www.wcc-group.com/page.aspx?menu=products_001&page=products_software (consultada el 16 de agosto de 2013).

¹⁸ Véase http://epic.org/privacy/carnivore/foia_documents.html (17 de agosto de 2013).

información, piratería y otros delitos graves que ocurren en Internet. Este sistema se implementó en 2000, hoy en día se ha perfeccionado.¹⁹

Inspección profunda de paquetes. Las empresas Siemens y Nokia elaboraron un programa denominado “centro de monitoreo”, el cual permite abrir los correos electrónicos, detectar mensajes con determinadas palabras en la Web y controlar masivamente el contenido de blogs. Este programa opera actualmente en Irán.

2. *Agentes animales*

Military Working Dogs (MWD). Estos perros, junto con sus manejadores, están desplegados en todo el mundo para ayudar a la policía y en operaciones militares. Los MWD han estado en la Segunda Guerra Mundial, en la guerra de Vietnam y recientemente en Afganistán; no sólo ayudan protegiendo las bases militares, sino que también detectan bombas, minas y droga.²⁰

US Navy Marine Mammal Programme. La armada norteamericana ha trabajado con mamíferos marinos desde 1950, cuando la armada comenzó a estudiar las características únicas de los mamíferos marinos, tales como la hidrodinámica de los delfines. Mediante el estudio de cómo los delfines se mueven en el agua, la marina perfeccionó el diseño de torpedos, barcos y submarinos. A diferencia de los buzos, los delfines son capaces de realizar continuas inmersiones profundas sin experimentar “las curvas” —enfermedad de descompresión—. Los delfines y leones marinos son animales de gran fiabilidad y adaptables, pero sobre todo a través de entrenamiento pueden buscar, detectar y marcar la ubicación de objetos en el agua.²¹

IV. DIVERSAS TECNOLOGÍAS UTILIZADAS PARA ACTIVIDADES DE SEGURIDAD NACIONAL

Aquí se desarrollan tecnologías utilizadas en actividades de seguridad nacional, las cuales abarcan las desde biométricas, químicas y biológicas, hasta las biotecnológicas y geofísicas.

¹⁹ Cfr. el testimonio de Donald M. Kerr, asistente del director del FBI, disponible en: http://www.au.af.mil/au/awc/awcgate/fbi/carnivore_tool.htm (consultada el 17 de agosto de 2013).

²⁰ Como ejemplo puede consultarse la descripción de la Real Fuerza Aérea Australiana: <http://www.airforce.gov.au/SFS/MWDTF/index.aspx> (consultada el 17 de agosto de 2013).

²¹ Para mayor información del programa véase la página oficial: <http://www.public.navy.mil/spawar/Pacific/71500/Pages/Animals.aspx> (consultada el 17 de agosto de 2013). La traducción es nuestra.

1. *Tecnología biométrica*

La biometría es una técnica automatizada que a través de características físicas y pautas de comportamiento identifica y verifica la identidad de las personas, animales y objetos.²² En este apartado nos centraremos en la identificación y verificación de personas. Las características biométricas más comunes son el rostro, iris,²³ huellas dactilares, características de la mano y voz, muestras biológicas (sangre, piel, células óseas o plasma sanguíneo), entre otras.

Los datos biométricos son datos personales sensibles y se les clasifica por el nivel de intrusión a la privacidad. Aunque hay datos biométricos que por sí solos no podrían identificar a una persona, al conjugarse dos o más datos biométricos, la identificación y verificación del titular de los datos elimina cualquier margen de error, pues se autentifica y reconoce que esa persona es quien dice ser.

No existe un tratado o convención internacional que verse sobre la información biométrica, y por ende la regulación depende de cada uno de los países que utilizan este tipo de tecnología. Generalmente la regulación recae en las leyes sobre privacidad y datos personales que contemplen la sistematización de la información, pero también el flujo de información tanto nacional como internacional.

Entre las aplicaciones de identificación se incluyen la identificación forense de huellas dactilares latentes, detección de sujetos en las famosas “listas negras” —terrorismo internacional, delincuencia organizada, etcétera— control fronterizo en las aduanas migratorias —a través de pasaportes y visas—, control de acceso a un recinto —sobre todo en áreas de máxima seguridad—, control de acceso a un sistema informático, control de identidad por las autoridades —a través de documentos nacionales de identidad—, utilización de servicios —cajeros automáticos, transporte público, asistencia a los lugares de trabajo, etcétera—, cobro de servicios —comercio electrónico, pago a distancia, etcétera—, utilización de dispositivos —teléfonos móviles, automóviles, etcétera—, redes sociales —Facebook, Google Picasa, etcétera—.

Hoy en día, los servicios policiales y de inteligencia elaboran dos tipos de perfiles biométricos. Los perfiles de tipo fisiológico incluyen los siguientes:

²² Hopkins, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law, Computers & Technology*, núm. 13, pp. 337-363.

²³ En el caso del iris, aunque es muy popular por las películas, no existe una gran cantidad de software y hardware que lo realicen con certeza, y ello conlleva a altos márgenes de error tanto en la captura de la información como en la lectura de la información.

identificación de huellas dactilares, reconocimiento del iris, reconocimiento de la retina, identificación de la geometría de la mano, reconocimiento de la geometría facial, reconocimiento mediante el uso de termogramas faciales, análisis de ADN, reconocimiento auricular, exploración del patrón venoso en la muñeca, etcétera. Entre los perfiles basados en comportamiento tenemos la identificación por la voz, reconocimiento de la firma, dinámica de pulsación en teclado, análisis del patrón de pisadas al caminar, etcétera.²⁴

2. *Tecnología química*

En esta sección nos referimos a las “armas químicas”. Aunque se tienen registros históricos de la existencia de flechas envenenadas, arsénico, entre otros,²⁵ oficialmente la existencia de armas químicas data de la Primera Guerra Mundial con los cartuchos lanzados que contenían gases de cloro y fosgeno. Para la Segunda Guerra Mundial las armas químicas se perfeccionaron. Actualmente, las antiguas armas químicas y las armas químicas abandonadas representan un problema real para los países.²⁶

Durante la Guerra Fría, Estados Unidos y la extinta Unión Soviética desarrollaron y conservaron arsenales de armas químicas. En las guerras de Iraq e Irán —en los años ochenta— se utilizaron el gas mostaza y agentes neurotóxicos. En 1994, Japón sufrió el envenenamiento en una zona residencial y ataques en el metro de Tokio (en 1995) con la sustancia sarín. Ahora bien, el término arma química se aplica a cualquier sustancia química tóxica, o a sus precursores, que puede causar la muerte, heridas, incapacidad temporal o irritación sensorial por su acción química. También se consideran armas las municiones o dispositivos destinados al lanzamiento de armas químicas, con carga o sin ella.²⁷

Cabe resaltar que la definición ofrecida por la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de

²⁴ Para información detallada sobre sistemas biométricos implementados tanto a nivel nacional como internacional se recomienda ver Díaz, Vanessa, “Sistemas biométricos en materia criminal: un estudio comparado”, *Revista IUS*, México, núm. 31, año VII, enero-junio de 2013, pp. 28-47.

²⁵ Por ejemplo, en la mitología griega personajes como Gerion y Paris pierden la vida por flechas envenenadas; mientras que los Borgia utilizaban venenos para acrecentar su poder.

²⁶ Véase <http://www.opcw.org/sp/novedades-y-publicaciones/publicaciones/fundamentos/> (consultada el 14 de agosto de 2013).

²⁷ *Cfr.* artículo II de la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su Destrucción (CAQ), disponible en: http://www.opcw.org/index.php?eID=dam_frontend_push&docID=6354 (consultada el 14 de agosto de 2013).

Armas Químicas y sobre su Destrucción (CAQ)²⁸ incluye no sólo las sustancias químicas, sino también los agentes neurotóxicos (gases nerviosos).

A continuación se presenta la clasificación de agentes químicos —sustancias químicas que tienen el potencial de causar cambios fisiológicos en los seres humanos y animales— bajo el concepto ofrecido por la CAQ:

- Agente asfixiante: clase de armas químicas diseminadas en forma de gas. Son absorbidas por los pulmones, donde causan una acumulación de fluidos y la asfixia de la víctima.
- Agente de represión de disturbios (ARD): cualquier sustancia química no enumerada en una Lista, que puede producir rápidamente en los seres humanos una irritación sensorial o efectos incapacitantes físicos que desaparecen en breve tiempo después de concluida la exposición al agente. La policía o las fuerzas armadas utilizan a menudo estas sustancias químicas para controlar a las multitudes.
- Agente discapacitante: Agente químico que produce una debilitación temporal física o psicológica, incapacitando así a un ser humano o animal para el desempeño normal de sus tareas o funciones.
- Agentes neurotóxicos: conocidos también como gases nerviosos. Componente organofosforado sumamente tóxico y potencialmente letal que afecta al sistema nervioso, inhibiendo la enzima que permite la transmisión de impulsos nerviosos. Una sola gota de un agente neurotóxico absorbida por la piel puede causar la muerte. Los agentes neurotóxicos pueden dispersarse en forma líquida o en aerosol, lo que permite su inhalación o absorción por vía cutánea. Los agentes neurotóxicos se dividen en dos familias: los agentes G y los agentes V.
 - Agente G: familia de agentes neurotóxicos entre los que se encuentran el tabún, el sarín y el somán.
 - Agente V: grupo de agentes neurotóxicos estables, que es unas diez veces más tóxico que el sarín. Se encuentran los VA, VG y el VX.
- Agentes hemotóxicos: categoría de armas químicas que se dispersan como gases y que son absorbidos por vía pulmonar. Afectan la capa-

²⁸ La Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su Destrucción (CAQ) es el primer tratado multilateral encargado de prohibir toda una categoría de armas de destrucción en masa (ADM). La CAQ consta de un preámbulo, 24 artículos y 3 anexos: el Anexo sobre Sustancias Químicas, el Anexo sobre Verificación y el Anexo sobre Confidencialidad. Disponible en: http://www.opcw.org/index.php?eID=dam_frontend_push&docID=6354 (consultada el 14 de agosto de 2013).

cidad de utilización del oxígeno por los hematíes y provocan falta de riego e incluso paro cardíaco.

- Agente vesicante: agente químico que afecta a la piel y en especial a las partes húmedas del cuerpo, como los ojos y las mucosas de los sistemas respiratorio y digestivo.

El anexo de la CAQ sobre sustancias químicas establece tres listas de sustancias químicas respecto a las que se prevé la aplicación de medidas de verificación a través de inspecciones por parte de la Organización para la Prohibición de Armas Químicas (OPAQ), cuya función principal es la supervisión de su destrucción y la no proliferación de armas químicas.²⁹

	<i>Lista 1</i>
A.	Sustancias químicas tóxicas
1.	Alkil (metil, etil, propil (normal o isopropil)) fosfonofluoridatos de 0-alkilo (<C10, incluido el cicloalkilo). Ej. Sarín: Metilfosfonofluoridato de 0-isopropilo (107-44-8). Somán: Metilfosfonofluoridato de 0-pinacolilo (96-64-0).
2.	N,N-dialkil (metil, etil, propil (normal o isopropil)) fosforamidocianidatos de 0-alkilo (<C10, incluido el cicloalkilo). Ej. Tabún: N,N-dimetilfosforamidocianidato de 0-etilo (77-81-6).
3.	S-2-dialkil (metil, etil, propil (normal o isopropil)) aminoetilalkil (metil, etil, propil (normal o isopropil)) fosfonotiolatos de 0-alkilo (H ó <C10, incluido el cicloalkilo) y sales alquilatadas o protonadas correspondientes. Ej. VX: S-2-diisopropilaminoetilmetilfosfonotiolato de 0-etilo (50782-69-9).
4.	Mostazas de azufre: Clorometilsulfuro de 2-cloroetil (2625-76-5). Gas mostaza: sulfuro de bis (2-cloroetilo) (505-60-2). Bis(2-cloroetiltio)metano (63869-13-6). Sesquimostaza: 1,2-bis(2-cloroetiltio)etano (3563-36-8). 1,3-bis(2-cloroetiltio)propano normal (63905-10-2). 1,4-bis(2-cloroetiltio)butano normal (142868-93-7). 1,5-bis(2-cloroetiltio)pentano normal (142868-94-8). Bis(2-cloroetiltio)metiléter (63918-90-1). Mostaza O: bis(2-cloroetiltio)éter (63918-89-8).

²⁹ Véase <http://www.opcw.org/sp/> (consultada el 14 de agosto de 2013).

5.	Lewisitas: Lewisita 1: 2-clorovinildicloroarsina (541-25-3). Lewisita 2: bis(2-clorovinil) cloroarsina (40334-69-8). Lewisita 3: tris(2-clorovinil) arsina (40334-70-1).
6.	Mostazas de nitrógeno: HN1: bis(2-cloroetil) etilamina (538-07-8). HN2: bis(2-cloroetil) metilamina (51-75-2). HN3: tris(2-cloroetil) amina (555-77-1).
7.	Saxitoxina (35523-89-8).
8.	Ricina (9009-86-3).
B.	Precursores
9.	Fosfonildifluoruros de alquilo (metilo, etilo, propilo (normal o isopropilo)). Ej. DF: metilfosfonildifluoruro (676-99-3).
10.	0-2-dialkil (metil, etil, propil (normal o isopropil)) aminoetilalkil (metil, etil, propil (normal o isopropil)) fosfonitos de 0-alkilo (H o <C10, incluido el cicloalkilo) y sales alquiladas o protonadas correspondientes. Ej. QL: 0-2-diisopropilaminoetilmetilfosfonito de 0-etilo (57856-11-8).
11.	Cloro Sarín: metilfosfonocloridato de 0-isopropilo (1445-76-7).
12.	Cloro Somán: metilfosfonocloridato de O-pinacolilo (7040-57-5).
<i>Lista 2</i>	
A.	Sustancias químicas tóxicas
1.	Amitón: Fosforotiolato de 0,0-dietil S-2-(dietilamino) etil y sales alquiladas o protonadas correspondientes (78-53-5).
2.	PFIB: 1,1,3,3,3-pentafluoro-2-(trifluorometil) de 1-propeno (382-21-8).
3.	BZ: Bencilato de 3-quinuclidinilo* (6581-06-2).
B.	Precursores
4.	Sustancias químicas, excepto las sustancias enumeradas en la Lista 1, que contengan un átomo de fósforo al que esté enlazado un grupo metilo, etilo o propilo (normal o isopropilo), pero no otros átomos de carbono. Ej. Dicloruro de metilfosfonilo (676-97-1). Metilfosfonato de dimetilo (756-79-6). Excepción: Fonofos: etilfosfonotiolotionato de O-etilo S-fenilo (944-22-9).

* Este tipo de sustancia química está sometida a umbrales especiales para la declaración y verificación según la parte VII del Anexo sobre Verificación de la CAQ.

5.	Dihaluros N,N-dialkil (metil, etil, propil (normal o isopropil)) fosforamídicos.
6.	N,N-dialkil (metil, etil, propil (normal o isopropil)) fosforamidatos dialkílicos (metílicos, etílicos, propílicos (propilo normal o isopropilo).
7.	Tricloruro de arsénico (7784-34-1).
8.	Acido 2,2-difenil-2-hidroxiacético (76-93-7).
9.	Quinuclidinol-3 (1619-34-7).
10.	Cloruros de N,N-dialkil (metil, etil, propil (normal o isopropil)) aminoetilo-2 y sales protonadas correspondientes.
11.	N,N-dialkil (metil, etil, propil (propilo normal o isopropilo)) aminoetanol-2 y sales protonadas correspondientes. Excepciones: N,N-dimetilaminoetanol y sales protonadas correspondientes (108-01-0). N,N-dietilaminoetanol y sales protonadas correspondientes (100-37-8).
12.	N,N-dialkil (metil, etil, propil (propilo normal o isopropilo)) aminoetanoltioles-2 y sales protonadas correspondientes.
13.	Tiodiglicol: sulfuro de bis (2-hidroxietilo) (111-48-8).
14.	Alcohol pinacolílico: 3,3-dimetilbutanol-2 (464-07-3).
<i>Lista 3</i>	
A.	Sustancias químicas
1.	Fosgeno: dicloruro de carbonilo (75-44-5).
2.	Cloruro de cianógeno (506-77-4).
3.	Cianuro de hidrógeno (74-90-8).
4.	Cloropicrina: tricloronitrometano (76-06-2).
B.	Precursores
5.	Oxicloruro de fósforo (10025-87-3).
6.	Tricloruro de fósforo (7719-12-2).
7.	Pentacloruro de fósforo (10026-13-8).
8.	Fosfito trimetílico (121-45-9).
9.	Fosfito trietilico (122-52-1).
10.	Fosfito dimetílico (868-85-9).

11.	Fosfito dietílico (762-04-9).
12.	Monocloruro de azufre (10025-67-9).
13.	Dicloruro de azufre (10545-99-0).
14.	Cloruro de tionilo (7719-09-7).
15.	Etildietanolamina (139-87-7).
16.	Metildietanolamina (105-59-9).
17.	Trietanolamina (102-71-6).

FUENTE: Anexo “Listas de sustancias químicas de la CAQ”.

3. *Tecnología biológica*

Las armas biológicas, al igual que las químicas, fueron utilizadas en la Primera y Segunda Guerra Mundial. Durante la Guerra Fría, los programas de armamento biológico se expandieron en países como Canadá, China, Corea del Norte, Cuba, Bulgaria, Egipto, Estados Unidos, India, Iraq, Irán, Israel, Japón, Laos, Reino Unido, Siria, Taiwán, Vietnam y la extinta Unión Soviética.

En 1972, oficialmente estos programas se detuvieron con la firma de la Convención sobre la Prohibición del Desarrollo, Producción y Almacenamiento y Destrucción de Armas Bacteriológicas (biológicas) y Tóxicas (CABT).³⁰ Sin embargo, la CABT no cuenta con un mecanismo de verificación ni organismo internacional que ejerza un control real de destrucción y no proliferación de armas biológicas.³¹

Las armas biológicas son organismos o toxinas que pueden matar o incapacitar a humanos y animales, a través del agua, el aire y la contaminación de alimentos en general. Los agentes biológicos utilizados como armas son las bacterias, virus y toxinas:

- Las bacterias son organismos microscópicos que viven libremente y que se reproducen por división simple y de fácil cultivo. Las enfermedades que producen a menudo responden al tratamiento con antibióticos.

³⁰ Se puede consultar el texto de la Convención en idioma inglés en: <http://www.opbw.org/convention/documents/btwcext.pdf> (consultada el 15 de agosto de 2013). Actualmente cuenta con 155 países que ratificaron la CABT y 16 países que están en proceso de firma.

³¹ Véase <http://www.opbw.org/> (consultada el 15 de agosto de 2013).

- Los virus requieren organismos vivientes para reproducirse, ya que no son seres vivos, son sólo información genética. Son como una especie de “parásitos” que dependen íntimamente del cuerpo que infectan. Los virus producen enfermedades que por lo general no responden a los antibióticos. No obstante, las drogas antivirales a veces son eficaces. Han existido programas de investigación genética para producir las llamadas quimeras, virus recombinados que tienen las características de varios antecesores.
- Las toxinas son sustancias venenosas que se encuentran y se extraen de plantas, animales o microorganismos vivos; algunas toxinas pueden producirse o alterarse por medios químicos. Algunas toxinas pueden tratarse con antitoxinas específicas y drogas selectas.

En 1984 se formó el Grupo de Australia,³² cuyo objetivo es el de garantizar, a través de medidas regulatorias de la exportación de determinadas sustancias químicas, agentes biológicos y elementos y equipos para la fabricación de sustancias químicas y biológicas de doble uso, que las exportaciones de dichos productos realizadas desde sus países no contribuyan a la proliferación de armas químicas y biológicas.³³

Actualmente, son 43 países, más la Comisión Europea, los que conforman el Grupo de Australia: Alemania, Argentina, Australia, Austria, Bélgica, Bulgaria, Canadá, República Checa, República de Chipre, República de Corea, Croacia, Dinamarca, República Eslovaca, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, Rumania, Suecia, Suiza, República de Turquía y Ucrania.

A continuación se presenta una lista básica de agentes biológicos elaborada por los Estados miembros del Grupo Australia:

LISTA DE AGENTES BIOLÓGICOS

<i>Bacterias</i>	<i>Virus</i>	<i>Toxinas</i>	<i>Hongos</i>
Clostridium tetani	Virus de los Andes	Toxinas botulínicas ⁴	Fusarium sporotrichioides
Legionella pneumophila	Virus de Chapare	Toxinas de Clostridium perfringens	Fusarium langsethiae

³² Véase <http://www.australiagroup.net/es/index.html> (consultada el 15 de marzo de 2013).

³³ Véase <http://www.australiagroup.net/es/objetivos.html> (consultada el 15 de marzo de 2013).

<i>Bacterias</i>	<i>Virus</i>	<i>Toxinas</i>	<i>Hongos</i>
Yersinia pseudo-tuberculosis	Virus Chikungunya	Conotoxina	Coccidioides immitis
Bacillus anthracis	Virus Choclo	Ricina	Coccidioides posadasii
Brucella abortus	Virus de la fiebre hemorrágica de Crimea-Congo	Saxitoxina	
Brucella melitensis	Virus del dengue	Toxina Shiga	
Brucella suis	Virus Dobrava-Belgrado	Toxinas de Staphylococcus aureus	
Chlamydomydia psittaci (antes llamada Chlamydia psittaci)	Virus de la encefalitis equina del Este	Tetrodotoxina	
Clostridium botulinum	Virus del Ébola	Verotoxina	
Francisella tularensis	Virus Guanarito	Microcistina (Cian- ginosina)	
Burkholderia mallei (Pseudomonas mallei)	Virus Hantaan	Aflatoxinas	
Burkholderia pseudomallei (Pseudomonas pseudomallei)	Virus Hendra (Morbilivirus equino)	Abrina	
Salmonella typhi	Virus de la encefalitis japonesa	Toxina colérica	
Shigella dysenteriae	Virus Junín	Toxina diacetoxiscirpenol	
Vibrio cholerae	Virus del bosque de Kyasanur	Toxina T-2	
Yersinia pestis	Virus Laguna Negra	Toxina HT-2	

<i>Bacterias</i>	<i>Virus</i>	<i>Toxinas</i>	<i>Hongos</i>
Clostridium perfringens, tipos productores de toxinas epsilon	Virus de Lassa	Toxina modecina	
Escherichia coli enterohemorrágica, serotipo 0157 y otros serotipos productores de verotoxina	Virus de Louping ill	Toxina volkensina	
Coxiella burnetti	Virus Lujo	Lectina 1 de Viscum album (Viscumina)	
Rickettsia prowazekii	Virus de la coriomeningitis linfocítica		
	Virus Machupo		
	Virus de Marburg		
	Virus de la viruela del mono		
	Virus de la encefalitis del Valle de Murray		
	Virus Nipah		
	Virus de la fiebre hemorrágica de Omsk		
	Virus Oropouche		
	Virus de Powassan		
	Virus de la fiebre del Valle del Rift		
	Virus Rocío		
	Virus Sabia		
	Virus de Seúl		
	Virus Sin Nombre		
	Virus de la encefalitis de San Luis		

<i>Bacterias</i>	<i>Virus</i>	<i>Toxinas</i>	<i>Hongos</i>
	Virus de la viruela		
	Virus de la encefalitis equina venezolana		
	Virus de la encefalitis equina del Oeste		
	Virus de la fiebre amarilla		

FUENTE: Lista de agentes biológicos del Grupo de Australia.

A continuación se presenta una lista básica de patógenos vegetales elaborada por los Estados miembros del Grupo Australia.

<i>Bacterias</i>	<i>Virus</i>	<i>Hongos</i>
<i>Xanthomonas alibilineans</i>	Tymovirus latente andino de la patata	<i>Colletotrichum coffeanum</i> var. <i>virulans</i> (<i>Colletotrichum kahawae</i>)
<i>Xanthomonas campestris</i> pv. <i>citri</i>	Viroide del tubérculo fusiforme de la patata	<i>Cochliobolus miyabeanus</i> (<i>Helminthosporium oryzae</i>)
<i>Xanthomonas oryzae</i> pv. <i>oryzae</i> (<i>Pseudomonas campestris</i> pv. <i>oryzae</i>)	Virus del “bunchy top” del banano	<i>Microcyclus ulei</i> (sin. <i>Dothidella ulei</i>)
<i>Clavibacter michiganensis</i> subsp. <i>sepedonicus</i> (<i>Corynebacterium michiganensis</i> subsp. <i>sepedonicum</i> o <i>Corynebacterium sepedonicum</i>)		<i>Puccinia graminis</i> (sin. <i>Puccinia graminis</i> f. sp. <i>tritici</i>)
<i>Ralstonia solanacearum</i> razas 2 y 3 (<i>Pseudomonas solanacearum</i> razas 2 y 3 o <i>Burkholderia solanacearum</i> razas 2 y 3)		<i>Puccinia striiformis</i> (sin. <i>Puccinia glumarum</i>)
<i>Xylella fastidiosa</i>		<i>Pyricularia grisea</i> / <i>Pyricularia oryzae</i>

<i>Bacterias</i>	<i>Virus</i>	<i>Hongos</i>
		Deuterophoma tracheiphila (sin. Phoma tracheiphila)
		Monilia rorei (sin. Monilophthora rorei)

FUENTE: Lista de patógenos vegetales del Grupo de Australia.

A continuación se presenta una lista básica de patógenos animales elaborada por los Estados miembros del Grupo Australia.

<i>Bacterias</i>	<i>Virus</i>
<i>Mycoplasma mycoides</i> , subsp. <i>mycoides</i> SC (colonia pequeña)	Virus de la peste porcina africana
<i>Mycoplasma capricolum</i> , subsp. <i>capripneumoniae</i> (“cepa F38”)	Virus de la influenza aviar ²
<i>Borrelia burgdorferi</i>	Virus de la lengua azul
	Virus de la fiebre aftosa
	Virus de la viruela caprina
	Virus del herpes (enfermedad de Aujeszky)
	Virus del cólera porcino (sinónimo: virus de la peste porcina)
	Virus de la rabia
	Virus de la enfermedad de Newcastle
	Virus de la peste de pequeños rumiantes
	Enterovirus porcino tipo 9 (sinónimo: virus de la enfermedad vesicular porcina)
	Virus de la peste bovina
	Virus de la viruela ovina
	Virus de la enfermedad de Teschen
	Virus de la estomatitis vesicular
	Virus de la dermatosis nodular
	Virus de la peste equina

FUENTE: Lista de patógenos animales del Grupo de Australia.

En este mismo sentido se destaca la lista básica de agentes biológicos contenida en un manual de operaciones elaborado de manera conjunta por la marina, la armada, la fuerza aérea y la guardia costera de los Estados Unidos de América.

Esta publicación ofrece la doctrina para ayudar a los comandantes y el personal en la planificación, la preparación, desarrollo y evaluación de las operaciones en las que sus fuerzas puedan encontrar armas químicas, biológicas, radiológicas y nucleares, amenazas y peligros. Estos principios se aplican en toda la gama de operaciones militares.³⁴

<i>Bacteria y Rickettsia</i>	<i>Virus</i>	<i>Toxinas</i>
Ántrax (<i>Bacillus anthracis</i>)	Viruela (<i>Variola mayor</i>)	Botulina (toxina botulínica)
Plaga (<i>Yersinia pestis</i>)	Encefalitis Viral Equina (tanto la del Este, Oeste y de Venezuela)	Ricina (<i>ricinus communis</i>)
Fiebre Q (<i>Coxiella burnetii</i>)	Fiebres hemorrágicas virales (virus del Ébola, virus de la fiebre del Valle del Rift, virus de Marburg, virus de Lassa, virus del dengue, etcétera)	Enterotoxina estafilocócica B
Tularemia (<i>Francisella tularensis</i>)		Micotoxinas tricotecenos (T2)

FUENTE: Joint Chief of Staff, *Operations in Chemical, Biological, Radiological and Nuclear (CBRN) Environments*, Estados Unidos, 26 de agosto de 2008, apéndice C.

La Organización del Tratado del Atlántico Norte (OTAN) contempla un listado de 31 agentes biológicos dentro de los que se destacan la viruela, el ántrax, la peste, el botulismo, la tularemia, el tifus, la fiebre Q, la encefalitis equina venezolana, el Ébola y la influenza.³⁵

4. Biotecnología: ingeniería genética

La biotecnología³⁶ es una técnica utilizada para la manipulación del material genético de los organismos vivos. En este apartado nos centrare-

³⁴ Joint Chief of Staff, *Operations in Chemical, Biological, Radiological and Nuclear (CBRN) Environments*, Estados Unidos, 26 de agosto de 2008, p. i, disponible en: http://www.dtic.mil/doctrine/new_pubs/jp3_11.pdf (consultada el 15 de abril de 2013). La traducción es nuestra.

³⁵ Véase <http://www.nato-pa.int/default.asp?SHORTCUT=2> (consultada el 15 de abril de 2013).

³⁶ La biotecnología presenta muchos campos de aplicación: terapéuticos, diagnósticos,

mos en dos de los proyectos sufragados por la *Defense Advanced Research Projects Agency* (DARPA) y realizados por universidades norteamericanas, como por ejemplo: la Universidad de California-Berkeley y el programa de sensores implantados a escarabajos cuyo director es el profesor Michel Maharbiz,³⁷ y el programa sobre manipulación de receptores biológicos de las plantas para la detección de explosivos, cuya directora es June Medford de la Universidad de Colorado.³⁸

5. *Tecnología geofísica*

Las técnicas de modificación ambiental tienen como objetivo alterar — mediante la manipulación deliberada de los procesos naturales — la dinámica, la composición o estructura de la Tierra, incluida su biótica, su litosfera, su hidrosfera y su atmósfera, o del espacio ultraterrestre.

La Convención sobre la Prohibición de Utilizar Técnicas de Modificación Ambiental con Fines Militares u otros Fines Hostiles (ENMOD, por sus acrónimos en inglés) es un instrumento de derecho internacional relacionado con el desarme, prohibiendo el empleo del medio ambiente como herramienta de combate.³⁹ Sin embargo, los programas —norteamericanos (HAARP) y rusos (SURA)— de investigación de Aurora Activa de Alta Frecuencia Utilizada han generado la expectativa de ser utilizados como armas de destrucción masiva (AMD).⁴⁰

Este tipo de programas se basan en experimentos de Nicolás Tesla, científico de las ondas de radio y electromagnetismo. Las antenas funcio-

alimentación, medio ambiente, etcétera. Los inicios de la biotecnología se remontan a Mendel en 1865, quien establece las bases de la genética.

³⁷ Singer, Emily, “TR10: Biological Machines”, *Technology Review*, marzo-abril de 2009, disponible en: <http://www.technologyreview.com/biomedicine/22111/> (consultada el 17 de abril de 2013); véase también <http://alt1040.com/2011/09/insectos-roboticos-espias-futuro> (consultada el 17 de abril de 2013).

³⁸ Véanse <http://wp.natsci.colostate.edu/medfordlab/> (consultada el 17 de abril de 2013) y <http://www.larazon.es/noticia/3940-ee-uu-modifica-geneticamente-plantas-que-cambian-de-color-ante-los-explosivos> (consultada el 17 de abril de 2013).

³⁹ El 10 de diciembre de 1976, la Asamblea General de la Organización de las Naciones Unidas (ONU), en su Resolución 31/72, adoptó el ENMOD. El instrumento internacional consta de diez artículos y un párrafo anexo que se añade al final del texto de la Convención. La introducción que hace la Asamblea General de la ONU al Convenio se refiere claramente a la Resolución 1722 (XVI) del 20 de diciembre de 1961, en la que reconoce la importancia y el interés de todos los países por el desarme. Véase <http://www.icrc.org/spa/resources/documents/misc/treaty-1976-enmod-convention-5tdm2l.htm> (consultada el 14 de abril de 2013).

⁴⁰ La Estación HAARP se encuentra cerca de Gakona, Alaska, mientras que la Estación SURA se ubica en Vasilursk, Rusia.

nan enviando una descarga electromagnética con dirección a la ionósfera; hacen que ésta se caliente y sirva como espejo para luego dirigir el rebote hacia su blanco.

En un principio, el objetivo de este tipo de programas era la elaboración de escudos antimisiles y para la comunicación con submarinos atómicos a gran profundidad; sin embargo, la amplia gama de aplicación de este tipo de tecnología abarca la provocación de lluvias, sequías, movimiento de nubes, incremento de tornados, provocación de rayos o relámpagos, generación de ondas sísmicas, incremento de tsunamis, entre otros.⁴¹

El Parlamento Europeo, en su resolución A4-0005/1999, señala que “pese a los convenios existentes, la investigación en el sector militar sigue basándose en la manipulación medioambiental como arma, tal y como pone, por ejemplo, de manifiesto el sistema HAARP con base en Alaska”.⁴² Por ello, más adelante en esa misma resolución solicita a los Estados miembros de la Unión Europea “integrar en su concepto de seguridad los objetivos de conservación del medio ambiente y desarrollo sostenible”.⁴³

V. SOCIEDAD PROACTIVA EN ACTIVIDADES DE VIDEO-VIGILANCIA

Como se mencionó anteriormente, una sociedad proactiva en actividades de video-vigilancia es una fase importante dentro del reposicionamiento del ciudadano como presupuesto básico de cualquier democracia.

Ahora bien, en las últimas décadas la búsqueda por la reforma del Estado y de la administración pública ha evocado términos como buen gobierno, gobernabilidad o nueva gestión pública o gobernanza o nueva gobernanza,⁴⁴ en aras de reposicionar al ciudadano como partícipe activo

⁴¹ Proyecto HAARP, disponible en: <http://www.haarp.alaska.edu/haarp/index.html> y Proyecto SURA, disponible en: <http://sura.nirfi.sci-nnov.ru/page2.html?height=1150&source>About.Sura/About.html> (consultadas el 14 de agosto de 2013).

⁴² Véase <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1999-0005+0+DOC+XML+V0//ES> (consultada el 14 de agosto de 2013).

⁴³ *Idem.*

⁴⁴ Desde mediados de los años noventa, especialmente en Europa, ha ido emergiendo un consenso creciente en torno a que la eficacia y la legitimidad del actuar público se fundamenta en la calidad de la interacción entre los distintos niveles de gobierno y entre éstos y las organizaciones empresariales y de la sociedad civil. Los nuevos modos de gobernar en que esto se plasma tienden a ser reconocidos como gobernanza, gobierno relacional o en redes de interacción público-privado-civil a lo largo del eje local/global. La reforma de las estructuras y procedimientos de las administraciones públicas pasan a ser consideradas desde la lógica de su contribución a las redes de interacción o estructuras y procesos de gobernanza. Comisión de las Comunidades Europeas, *La gobernanza europea. Libro Blanco*, Bruselas, 2001.

en el gobierno. Para algunos tratadistas, estos términos no son sinónimos aunque sí complementarios unos de otros.⁴⁵ Sin embargo, lo que aquí interesa es que a estos tratadistas se les ha vuelto prioritario buscar respuestas a preguntas como: “¿gobiernan los gobiernos?, ¿cuáles son las condiciones que hacen posible que los gobiernos estén en aptitud de gobernar?, ¿cómo ajustar a las fuerzas armadas, la policía y los servicios de inteligencia en las nuevas democracias?”, entre otros.

Es más, en términos generales, la “gobernanza” sirve para comprender positivamente y reformar normativamente la estructura y procesos de administración —gobierno— en todos aquellos ámbitos en que la burocracia o la nueva gerencia pública resultan inapropiadas. Dichos ámbitos incluyen, desde luego, todas las actuaciones públicas relacionadas con los temas más complejos, diversos y dinámicos de nuestro tiempo, como son los servicios de inteligencia y seguridad nacional.⁴⁶

Ahora bien, el gran desafío de la gobernanza en materia de seguridad nacional es reestructurar las responsabilidades, tareas y actividades de cada una de las instituciones, organizaciones y entidades que integran y participan en el ámbito de seguridad nacional.⁴⁷

Lo anterior, plantea exigencias importantes de rediseño organizacional, de personal, de procedimientos, de instrumentos de gestión y presupuesto, de transparencia y de responsabilidad en materia de seguridad nacional.⁴⁸

Hay quien señala que el enfoque de gobernanza o nueva gestión pública es estrictamente gubernamental, dejando fuera a la sociedad, ya que se enfoca a condiciones y comportamientos del gobierno; no obstante, esa postura es errónea, pues el objetivo de este “movimiento” —sin importar el nombre que se utilice— es construir un gobierno capaz para sus gobernados.⁴⁹

⁴⁵ Nos referimos a Crozier, Huntington, Watanuki, Weber, Ptrats, Jacquet, Pisani-Ferry, Tubiana, Calame, Marin, Scholte, Stiglitz, entre otros.

⁴⁶ Cfr. Inter-Parliamentary Forum on Security Sector Governance in Southeast Asia (IPF-SSG-SEA), “Special Issue on «Parliamentary Accountability and Security Sector Governance in Southeast Asia»”, *Dialogue and Cooperation*, núm. 3, 2006, p. 5. También véase Villanueva, Ernesto, *Transparencia y declaración patrimonial de los servidores públicos: alcances y límites del derecho a saber*, México, Editora Periodística y Análisis de Contenidos- Editorial e, 2008.

⁴⁷ Cfr. Cerrillo I Martínez, Agustín (coord.), *La gobernanza hoy: 10 textos de referencia*, España, Ministerio de Administraciones Públicas, Instituto Nacional de Administración Pública, 2005, en Villanueva, Ernesto, *Transparencia y declaración patrimonial de los servidores públicos: alcances y límites del derecho a saber*, cit. Cfr. Inter-Parliamentary Forum on Security Sector Governance in Southeast Asia (IPF-SSG-SEA), “Special Issue on «Parliamentary Accountability and Security Sector Governance in Southeast Asia»”, cit., p. 5.

⁴⁸ *Idem*.

⁴⁹ Cfr. Aguilar, Luis F., “El aporte de la política pública y la nueva gestión pública a la

Sin embargo, este reposicionamiento del ciudadano no es una invención u ocurrencia; al contrario, es un presupuesto básico en cualquier democracia. Veamos.

Primero. El Estado constitucional democrático se basa en dos pilares fundamentales; por un lado, el reconocimiento de las libertades públicas como limitante al poder público y, por el otro, el establecimiento de controles internos y externos de la administración pública.

Es por ello que "...el sector de la seguridad... debería estar sometido a las mismas exigencias de eficacia, de igualdad y de responsabilidad que cualquier otro servicio público".⁵⁰ De lo contrario, el Estado no podría llevar a cabo sus funciones en condiciones de eficiencia, eficacia, equidad, legalidad, legitimidad y proporcionalidad.

Segundo. Bajo este supuesto, explica Miguel Acosta Romero que "el concepto de control externo e interno, se refiere a los procedimientos administrativos de gestión, evaluación, gasto público y cumplimiento de la legalidad...".⁵¹ Y comenta que "...no existe... una clasificación sobre lo que puede considerarse como control externo e interno, pues aquél puede hacer referencia o bien a la intervención de alguno de los poderes de la Unión, o al llamado control de constitucionalidad".⁵²

Aunado a lo anterior, Diego Valadés señala que un denominador común en los Estados constitucionales es el control eficiente del poder para garantizar el espacio de libertades individuales y colectivas, y la equidad entre los miembros de la colectividad.⁵³

Tercero. La doctrina en derecho comparado lo llama "control de constitucionalidad", que es una atribución propia del Estado. Es decir, el Estado sería el único que puede "regular con voluntad propia la misma Constitución"⁵⁴ o

gobernanza", conferencia presentada en el XII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santo Domingo, República Dominicana, octubre-noviembre de 2007.

⁵⁰ Annan, Kofi, "Peace and Development —One Struggle, Two Fronts", *Discurso del secretario general de las Naciones Unidas dirigido a miembros del Banco Mundial*, Organización de las Naciones Unidas, 19 de octubre de 1999, p. 5.

⁵¹ Acosta Romero, Miguel, *Teoría general del derecho administrativo*, México, Porrúa, 1991, pp. 514 y 515.

⁵² *Idem.*

⁵³ *Cfr.* Valadés, Diego, *El gobierno de gabinete*, México, UNAM, 2003, p. 2.

⁵⁴ *Ibidem*, p. 345. Bien señala Eduardo García que "la Constitución como instrumento jurídico ha de expresarse, precisamente, el principio de la autodeterminación política comunitaria, que es presupuesto del carácter originario y no derivado de la Constitución, así como el principio de la limitación del poder. Ninguno de los dos, y por supuesto no el último,

“autogobierno del pueblo, decisión autónoma sobre sus propios asuntos”,⁵⁵ o también “control parlamentario como control político”.⁵⁶ Por ende, en cualquier democracia⁵⁷ es necesario que los Estados establezcan tanto controles internos como externos dentro de la administración pública, más aún tratándose de seguridad nacional.

Cuarto. Los controles internos son todas aquellas normas, mecanismos, valores y principios que se implementan desde la estructura interna de cada una de las instituciones, organizaciones y dependencias que participan o realizan funciones en materia de seguridad nacional. Los controles externos son todas aquellas normas jurídicas, mecanismos y principios que se implementan a través de los poderes judicial y legislativo, así como también los ciudadanos a partir de la participación social o cohesión social (auditorías sociales) a todas las instituciones y entidades que participan en actividades de seguridad nacional —tanto de defensa como de inteligencia—.

Ahora bien, el reposicionamiento del ciudadano está basado en la búsqueda de la participación ciudadana; pero en un sentido más activo, dejando atrás la representación de partidos.⁵⁸ El reposicionamiento no sólo busca

son accesorios, sino esenciales”. García de Enterría, Eduardo, *La Constitución como norma y el Tribunal Constitucional*, Madrid, Civitas, 2006, p. 45.

⁵⁵ Böckenförde, Ernst Wolfgang, *Estudios sobre el Estado de derecho y la democracia*, Madrid, Trotta, p. 133.

⁵⁶ Aragón, Manuel, *Constitución, democracia y control*, México, UNAM, 2002.

⁵⁷ Desde los griegos hasta Rousseau se visualizaba a la democracia como democracia directa, en la cual los ciudadanos ejercen el derecho a la participación en la toma de decisiones sin intermediación. La democracia se asocia desde entonces con soberanía popular, voluntad general e interés común.

En el concepto de democracia moderna —a diferencia de los antiguos— se incorpora el tema de la división entre la titularidad y el ejercicio del poder, el principio de la mayoría, el constitucionalismo y la representación política.

Esta concepción tradicional de la democracia se articula en torno al protagonismo central del pueblo, concebido como soberano, como un todo homogéneo y capaz de producir una voluntad colectiva, potencializando su libertad a través de la juridificación de la soberanía. Bien señala Salvador Nava Gomar: “La democracia implica la constante posibilidad de modificar cualquier cosa, y esa opción se hace jurídicamente viable en el texto constitucional”. También señala que: “la democracia es un anhelo de las sociedades civilizadas”. Nava Gomar, Salvador, “El Estado constitucional: sinonimia positivizada entre Constitución y democracia (triple relación)”, *Anuario de Derecho Constitucional Latinoamericano*, México, 2003, p. 14.

⁵⁸ Held, David, *Modelos de democracia*, 2a. ed., Madrid, Alianza Editorial; Cunil, Nuria, “Repensando lo público a través de la sociedad: nuevas formas de gestión pública y representación social”, *Administración y Desarrollo*, núm. 37, 2002, pp. 122-126; Sartori, Giovanni, “En la defensa de la representación política”, *Revista Claves de Razón Práctica*, núm. 91, 1999; Laporta, Francisco J., “El cansancio de la democracia”, *Revista Claves de Razón Práctica*, núm. 99, 2000.

“una mayor incorporación de los ciudadanos al debate y a la deliberación de las políticas públicas”,⁵⁹ sino impulsar mecanismos de coparticipación y corresponsabilidad entre el gobierno, el sector privado —industrias que producen equipo y tecnología militar— y los ciudadanos en diferentes rubros, incluido el de seguridad nacional.

El avance tecnológico ha permitido que la sociedad pueda realizar actividades de vigilancia desarrolladas fundamentalmente por el Estado. Las actividades de vigilancia se han desarrollado por el impulso simultáneo de la proliferación de la tecnología y de los progresos de la cienciometría.

En este apartado mencionaremos algunos proyectos de video-vigilancia que actualmente se encuentran en operación y cuya información puede ser utilizada para actividades de seguridad nacional. Dos de las características en la elección de proyectos es, por un lado, la participación de centros de investigación y/o sociedad y, por el otro, que la información obtenida es utilizada para el desarrollo de tecnología en servicios de inteligencia.

- Sistema de Observación Terrestre (EOS, por sus acrónimos en inglés) operado por la NASA. EOS está compuesto por una serie de satélites coordinados en las orbitas polares; estos satélites están diseñados para monitorear los componentes claves del sistema climático y comprender sus interacciones a través de observaciones a largo plazo a nivel mundial (<http://eosps0.gsfc.nasa.gov/>).
- Censo de Vida Marina (Census of Marine Life) es una organización mundial cuyo objetivo es estimular el conocimiento de la vida marina a través de la investigación y análisis. Desde 2010 ha llevado a cabo diecisiete proyectos, de entre ellos destaca el proyecto OBIS (<http://www.coml.org/global-marine-life-database-obis>).
- El Sistema Océánico de Información Biográfica (OBIS, por sus acrónimos en inglés) es un sistema de información internacional sobre biodiversidad marina. Proporciona datos científicos geo-referenciados de las especies marinas; actualmente contiene cerca de 30 millones de registros geo-referenciados perfectamente identificados de especies de más de 800 bases de datos (a septiembre de 2010) (<http://www.iobis.org/>).
- Monitoreo Marino es operado por la Red de Monitoreo Marino (OTN, por sus acrónimos en inglés). El objetivo es recopilar datos

⁵⁹ Laporta, Francisco J., “El cansancio de la democracia”, *op. cit.*, p. 21.

completos sobre animales marinos en relación con el cambio de las propiedades físicas del océano. A pesar de su sofisticada tecnología, el seguimiento es bastante simple. Los científicos etiquetan una amplia gama de especies acuáticas —desde salmón, atún, ballenas, tiburones, pingüinos, cangrejos, entre otros— con pequeños transmisores electrónicos que se implantan quirúrgicamente o fijados externamente. Las etiquetas y receptores pueden ser equipados con sofisticados sensores que miden la temperatura del océano, la profundidad, salinidad, corrientes, química y otras propiedades (<http://oceantrackingnetwork.org/index.html>).

- Smithsonian Wild, operado por el Instituto Smithsonian. Su objetivo es estudiar la diversidad de la vida silvestre a través de video cámaras en una amplia gama de hábitats en todo el mundo. Actualmente cuenta con nueve proyectos, se destacan el Amazon Rainforest y Panama Palm Tree Survey (<http://siwild.si.edu/about.cfm>).
 - *Amazon Rainforest Peru*. Los objetivos del proyecto son: 1) realizar un inventario de las especies de mamíferos en una región no estudiada con anterioridad de la Amazonia peruana, y 2) investigar el impacto de carnívoros, en especial del ocelote (*Leopardus pardalis*) en la exploración de petróleo (<http://nationalzoo.si.edu/SCBI/MAB/research/arabela/default.cfm>).
 - *Panama Palm Tree Survey*. El objetivo es determinar la comunidad de mamíferos que se alimentan de dos especies de palmeras: *Attalea butyracea* o *standleyanum Astrocaryum*. Algunas cámaras también se instalaron en los árboles para registrar a los animales arborícolas que se alimentan de estos frutos (<http://agoutienterprise.wordpress.com>).
- Coalición Fronteriza de Alguaciles de Texas (TBSC, por sus acrónimos en inglés) es una asociación público-privada para implementar la vigilancia de la frontera de Texas en la comunidad virtual en tiempo real, a través de la participación de ciudadanos (<http://www.blueservo.net/about.php>).

La información recolectada por estos proyectos ayuda en la comprensión y desarrollo de productos y tecnologías utilizados en actividades de inteligencia y defensa.

VI. CONCLUSIONES

El tema de servicios de inteligencia y contrainteligencia es complejo y de actual coyuntura, que debe ser estudiado con enfoques multidisciplinarios. Más aún tratándose de la tecnología implementada para realizar dichas actividades. Hoy más que nunca, las actividades en materia de seguridad nacional deben someterse a lo que la doctrina llama “supremacía civil”; es decir, reposicionar al ciudadano como verdadero soberano de un Estado constitucional democrático. Por lo que las actividades de seguridad nacional tendrían las mismas exigencias de eficacia, de igualdad y de responsabilidad que cualquier otro servicio público.⁶⁰

Hoy en día existen diferentes programas y/o proyectos de carácter civil que con la información recolectada ayudan no sólo en la comprensión y desarrollo de productos, sino también en el desarrollo de tecnologías utilizadas en actividades de inteligencia y defensa.

Sin duda, el desarrollo tecnológico de las últimas décadas ha permitido un avance significativo en áreas de inteligencia y contrainteligencia. Este trabajo, por un lado, se centra en la clasificación de productos y tecnologías utilizadas en actividades de inteligencia y de defensa. Esto sin duda es de real importancia por considerar que pocos estudios identifican el producto o tecnología con la empresa que los desarrolla y diseña. Mientras que, por el otro, describe —de manera enunciativa más no limitativa— las tecnologías: químicas, biológicas, geofísicas y biométricas.

VII. BIBLIOHEMEROGRAFÍA

ACOSTA ROMERO, Miguel, *Teoría general del derecho administrativo*, México, Porrúa, 1991.

AGÜERO PIWONKA, Felipe, “Democracia en España y supremacía civil”, *Revista Española de Investigaciones Sociológicas*, núm. 44, 1988.

———, *Militares, civiles y democracia*, Madrid, Alianza Editorial, 1995.

AGUILAR, Luis, F., “El aporte de la política pública y la nueva gestión pública a la gobernanza”, conferencia presentada en el XII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santo Domingo, Republica Dominicana, octubre-noviembre de 2007.

ARAGÓN, Manuel, *Constitución, democracia y control*, México, UNAM, 2002.

⁶⁰ Annan, Kofi, “Peace and Development –One Struggle, Two Fronts”, *op. cit.*, p. 5.

- BAN, Ki-Moon, “Securing Peace and Development: The Role of the United Nations in Supporting Security Sector Reform”, *Reporte del Secretario General de las Naciones Unidas 2008*, Organización de las Naciones Unidas.
- BÖCKENFÖRDE, Ernst Wolfgang, *Estudios sobre el Estado de derecho y la democracia*, Madrid, Trotta.
- CENTRO PARA LA SEGURIDAD, EL DESARROLLO Y EL ESTADO DE DERECHO, *Política de seguridad nacional*, Ginebra, DCAF, 2008.
- , *Servicios de inteligencia*, Ginebra, DCAF, 2008.
- CLANCEY, Garner y LULHAM, Rohan, “Natural Surveillance”, conferencia presentada en *The Surveillance in/and Everyday Life Conference*, Universidad de Sydney, Australia, 20-21 de febrero de 2012.
- COMISIÓN DE LAS COMUNIDADES EUROPEAS, *La gobernanza europea. Libro Blanco*, Bruselas, 2001.
- COMISIÓN DE LIBERTADES CIVILES, JUSTICIA Y ASUNTOS DE INTERIOR DEL PARLAMENTO EUROPEO, *Documento de trabajo sobre una decisión del Consejo relativa a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza*, Parlamento Europeo, 10 de abril de 2007, DT\660824ES.doc, disponible en: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824es.pdf (consultada el 16 de agosto de 2013).
- DEL ÁGUILA, Rafael, “La democracia”, *Manual de ciencia política*, Madrid, Trotta.
- EUROPEAN COMMISSION, *Biometrics in Europe, Trend Report 2007*.
- GARCÍA DE ENTERRÍA, Eduardo, *La Constitución como norma y el Tribunal Constitucional*, Madrid, Civitas, 2006.
- HAGGERTY, Kevin D. y ERICSON, Richard V. (eds.), *The New Politics of Surveillance and Visibility*, Canadá, University of Toronto Press, 2006.
- HELD, David, *Modelos de democracia*, 2a. ed., Madrid, Alianza Editorial.
- HOPKINS, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law, Computers & Technology*, núm. 13.
- INTER-PARLIAMENTARY FORUM ON SECURITY SECTOR GOVERNANCE IN SOUTHEAST ASIA (IPF-SSG-SEA), “Special Issue on «Parliamentary Accountability and Security Sector Governance in Southeast Asia»”, *Dialogue and Cooperation*, núm. 3, 2006.
- JANOWITZ, Morris, *The Professional Soldier: A Social and Political Portrait*, A Free Press Paperback, 1964.

- JOINT CHIEFF OF STAFF, *Operations in Chemical, Biological, Radiological and Nuclear (CBRN) Environments*, Estados Unidos, 26 de agosto de 2008.
- JOHNSON, Loch K., “Ethical Intelligence: A Contradiction in Terms?”, *Intelligence and National Security*, 24 de junio de 2009.
- , “Preface to a Theory of Strategic Intelligence”, *International Journal of Intelligence and Counterintelligence*, núm. 16, invierno de 2003-2004.
- , *Bombs, Bugs, and Thugs: Intelligence and America’s Quest for Security*, Estados Unidos, New York University Press, 2002.
- , *National Security Intelligence: Secret Operations in Defense of the Democracies*, Cambridge, Polity, 2012.
- (ed.), *The Oxford Handbook of National Security Intelligence*, Estados Unidos, Oxford University Press, 2010.
- y WIRTZ, James, *Intelligence and National Security: The Secret World of Spies—An Anthology*, 2a. ed., Estados Unidos, Oxford University Press, 2007.
- KOFI, Annan, “Peace and Development —One Struggle, Two Fronts”, *Discurso del Secretario General de las Naciones Unidas dirigido a miembros del Banco Mundial*, Organización de las Naciones Unidas, 19 de octubre de 1999.
- KOHN, Richard H., “How Democracies Control the Military”, *Journal of Democracy*, vol. 8, núm. 4, 1997.
- NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, *Privacy & Biometrics Building a Conceptual Foundation*, Estados Unidos, The President of the United States Executive Office, 2006.
- NAVA GOMAR, Salvador, “El Estado constitucional: sinonimia positivizada entre Constitución y democracia (triple relación)”, *Anuario de Derecho Constitucional Latinoamericano*, México, 2003.
- NINO, Carlos, *La constitución de la democracia deliberativa*, Barcelona, Gedisa, 1997.
- LYON, David, “Cyberspace Sociality: Controversies over Computer-Mediated Communication”, en LOADER, B. (ed.), *The Governance of Cyberspace*, Londres, Nueva York, Routledge, 1997.
- , “Facing the Future: Seeking Ethics for Everyday Surveillance”, *Information Technology and Ethics*, 2001.
- , “Surveillance after September 11 2001”, *Sociological Research Online*, núm. 6, 2001.
- , *Surveillance Society: Monitoring Everyday Life*, Buckingham, Open University Press, 2001.

———, *The Electronic Eye: The Rise of Surveillance Society*, Cambridge, Polity Press, 1994.

VALADÉS, Diego, *El gobierno de gabinete*, México, UNAM, 2003.

VILLANUEVA, Ernesto, *Transparencia y declaración patrimonial de los servidores públicos: alcances y límites del derecho a saber*, México, Editora Periodística y Análisis de Contenidos-Editorial e, 2008.