Revista Científica General José María Córdova
ISSN: 1900-6586
ISSN: 2500-7645
Escuela Militar de Cadetes "General José María Córdova"

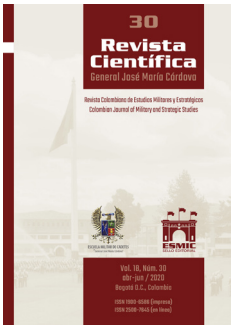
Cujabante Villamil, Ximena Andrea; Bahamón Jara, Martha Lucía;
Prieto Venegas, Jair Camilo; Quiroga Aguilar, Jorge Alejandro

Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares

Revista Científica General José María Córdova, vol. 18, núm. 30, 2020, Abril-Junio, pp. 357-377
Escuela Militar de Cadetes "General José María Córdova"

DOI: https://doi.org/10.21830/19006586.588

Disponible en: https://www.redalyc.org/articulo.oa?id=476268197006



Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares

Ximena Andrea Cujabante Villamil
https://orcid.org/0000-0002-5473-163X
ximena.cujabante@unimilitar.edu.co
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Martha Lucía Bahamón Jara
https://orcid.org/0000-0002-5877-6886
martha.bahamon@unimilitar.edu.co
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Jair Camilo Prieto Venegas
https://orcid.org/0000-0002-5894-443X
u0901636@unimilitar.edu.co
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Jorge Alejandro Quiroga Aguilar
https://orcid.org/0000-0002-9494-7574
u0901898@unimilitar.edu.co
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Citación: Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, *18*(30), 357-377. http://dx.doi.org/10.21830/19006586.588

Publicado en línea: 1.º de abril de 2020

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

Miles Doctus

Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

Volumen 18, número 30, abril-junio 2020, pp. 357-377
http://dx.doi.org/10.21830/19006586.588

Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares

Cybersecurity and cyber defense in Colombia: a possible model for civil-military relations

Ximena Andrea Cujabante Villamil, Martha Lucía Bahamón Jara, Jair Camilo Prieto Venegas y Jorge Alejandro Quiroga Aguilar
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Resumen. Este artículo se propone explorar el desarrollo institucional acerca del dominio del ciberespacio en Colombia y su incidencia sobre las relaciones cívico-militares en el país. Para ello, recurre a un análisis de fuentes primarias y secundarias, con el propósito de definir el ciberespacio y las ciberamenazas que surgen en él, así como describir las relaciones cívico-militares en Colombia y explicar el marco institucional referente a la seguridad y defensa del ciberespacio en el país. En este caso, y en contraste con la tradición del país, se evidencia que la iniciativa surgió del sector civil, lo que promovió una mayor participación de este sector en el campo de la seguridad y defensa. Así, la agenda de ciberseguridad y ciberdefensa puede ser la punta de lanza para replantear las relaciones cívico-militares.

Palabras clave: cibercrimen; ciberdefensa; cibernética; ciberseguridad; relaciones cívico-militares; seguridad de los datos

Abstract. This article explores the institutional development of the cyberspace domain in Colombia and its impact on civil-military relations in the country. An analysis of primary and secondary sources is used to define cyberspace and identify the cyber threats within it. It also describes civil-military relations in Colombia and the institutional framework of national cyberspace security and defense. Contrary to convention, in this case, it is evident that the initiative emerged from the country's civil sector, promoting greater participation of this segment in the field of security and defense. Thus, the cybersecurity and cyber defense agenda can be used to spearhead the rethinking of civil-military relations.

Keywords: civil-military relations; cybercrime; cyber defense; cybernetics; cybersecurity; data security

Sección: Seguridad y defensa • Artículo de investigación científica y tecnológica

Recibido: 13 de enero de 2020 • Aceptado: 14 de marzo de 2020

Contacto: Ximena Andrea Cujabante Villamil ximena.cujabante@unimilitar.edu.co

Introducción

La cuarta revolución industrial ha profundizado la globalización a causa de la masificación de internet y el creciente acceso a esta por parte de múltiples actores, al igual que la expansión de las relaciones humanas a entornos digitales no convencionales. Esto ha derivado en la creación del *ciberespacio* (Singer & Friedman, 2014). Allí, este entramado de relaciones trae consigo tanto oportunidades para el desarrollo de las sociedades como nuevas amenazas para los distintos colectivos humanos (Fernández, 2018; Schwab, 2016). Debido a ello, se ha dado paso a la participación de instituciones en el espacio cibernético, y ha surgido la necesidad de crear mecanismos para hacer frente a estas nuevas amenazas por parte de los Estados nacionales (Gücüyener, 2017).

El dominio del ciberespacio fue una carrera iniciada por las grandes potencias como Rusia, Estados Unidos y China, que por ello son un punto de referencia para la creación de instrumentos que salvaguarden la seguridad y la defensa nacional en el ciberespacio (Gaitán, 2018). En este sentido, Colombia, país pionero en la región, creó dos grandes lineamientos de política pública para el dominio del ciberespacio y salvaguardar su seguridad y defensa (Conpes 3854, 2016). En primer lugar, el Conpes 3701 de 2011 creó los lineamientos de ciberseguridad y ciberdefensa, que se fundamentan en la creación de nueva normatividad y organismos operativos para contrarrestar las amenazas existentes en el ciberespacio. Posteriormente se estructuró el Conpes 3854 de 2016, que, bajo el enfoque de gestión del riesgo, fundamenta la política de seguridad digital y complementa el Conpes anterior al poner énfasis en la maximización de las oportunidades existentes en el ciberespacio para el desarrollo de la sociedad y la economía colombiana, involucrando en la gestión del riesgo la multiplicidad de actores que intervienen en el ciberespacio y en la estructuración de una política de seguridad digital.

En Colombia, el desarrollo académico referente a los temas de ciberseguridad y ciberdefensa se ha centrado en un análisis de la regulación normativa e institucional de dinámicas variadas presentes en el ciberespacio, y ha dejado de lado el nivel de autonomía que han tenido las fuerzas militares en la gestión de seguridad y defensa en el ciberespacio. Dicha autonomía siempre ha estado supeditada a un control por parte del poder civil, que se establece por medio de instituciones jurídicas y políticas que garantizan un equilibrio para la conducción del Estado y la especialidad de sus funciones correspondientes. Sin embargo, debido a que las nuevas amenazas debilitan el marco establecido, estas reglas requieren de un proceso constante de revisión y construcción con el fin de hacer frente de manera oportuna a dichas amenazas (Burton, 2015).

En este sentido, para hacer frente a estas nuevas amenazas en Colombia, el poder civil, en cabeza del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) tiene la responsabilidad de establecer los lineamientos en materia de seguridad y defensa frente a las nuevas amenazas cibernéticas a la seguridad nacional. Esto socava la

autonomía histórica del sector defensa en la administración de seguridad y defensa nacional (Contreras, 2019).

Teniendo en cuenta lo anterior, el propósito de este artículo es explorar el desarrollo institucional del dominio del ciberespacio en Colombia y su incidencia sobre las relaciones cívico-militares en el país. En este orden de ideas, se parte de una conceptualización de lo que se entiende por ciberespacio y las amenazas a la seguridad y defensa nacional en este llamado quinto dominio. Posteriormente, se describe cómo han sido las relaciones cívico-militares en Colombia, al igual que el marco institucional referente a la seguridad y defensa en el ciberespacio. Finalmente se ofrecen algunas conclusiones.

Este artículo es de tipo descriptivo, ya que se apoya en técnicas de investigación cualitativa por medio de la recolección y análisis de fuentes primarias y secundarias que permiten describir el tema planteado. Asimismo, es de carácter exploratorio, debido a que es un tema poco abordado, por lo cual aspira a servir como un acercamiento inicial y una fuente de insumos para futuras investigaciones.

El ciberespacio como escenario de guerra o conflicto

El concepto de ciberespacio

Desde la primera revolución industrial, las economías han basado su progreso y bienestar en políticas industriales que se caracterizan según el momento histórico, lo que conlleva nuevos paradigmas tecnológicos y metodológicos. Estos procesos han tenido factores esenciales como la formación del talento humano, el avance de capacidades científicas y tecnológicas, el crecimiento de la autonomía económica regional, además de la creación de instituciones y sistemas nacionales de innovación, todo con el fin de impulsar de manera sostenida la transformación de la economía, el comercio internacional y el bienestar social. Estas políticas productivas responden principalmente a un proyecto nacional de desarrollo de vigencia continua (Acosta, 2016).

Desde finales del siglo XX y lo que se lleva del siglo XXI, el contexto internacional se ha caracterizado por una hiperglobalización impulsada gracias a la aparición de la tecnología digital, lo que ha provocado profundas transformaciones sociales, políticas y económicas a un acelerado ritmo (Fernández, 2018). Esto es reflejo de la revolución en marcha que están experimentando las sociedades contemporáneas, denominada como cuarta revolución industrial o Revolución 4.0, e identificada con la existencia de miles de millones de personas conectadas mediante dispositivos móviles. Dicha revolución ha dado lugar a "un poder de procesamiento, una capacidad de almacenamiento y un acceso al conocimiento sin precedentes" (Schwab, 2016, p. 9).

Esto ha sido posible por el incremento masivo de invenciones tecnológicas que comprenden varios campos como la robótica, el internet de las cosas (IoT), la inteligencia artificial (IA), el *big data*, los vehículos autónomos, la impresión 3D, la ciencia de materiales, la nanotecnología, la biotecnología, el almacenamiento de energía y la computación

cuántica, por nombrar los más destacados. Asimismo, se proyecta que la construcción y amplificación interrelacionada de estas tecnologías tenderá a modificar y fusionar las barreras de los mundos físico, digital y biológico. (Observatorio de Educación Superior de Medellín, 2019; Schwab, 2015).

Para Klaus Schwab, esta revolución se caracteriza, en primer lugar, porque se está desarrollando a un ritmo exponencial, como resultado de un mundo más interconectado y polifacético. En segundo lugar, se destaca la amplitud y profundidad de la revolución digital, que, en combinación con las innovaciones tecnológicas, ocasiona de forma acelerada cambios paradigmáticos sin precedentes en las relaciones internacionales, la economía, los negocios, la sociedad, el gobierno y las personas, modificando el qué y el cómo se hacen las cosas, e incluso quiénes somos. Por último, están las profundas transformaciones y el impacto en los sistemas de producción, en los gobiernos y la acción estatal interna y externa, así como en las empresas, industrias y la sociedad en su conjunto.

Sin embargo, este proceso no es únicamente tecnológico, también es una revolución cultural, debido a la misma hiperglobalización en la que, de forma paralela, cobran importancia temas locales. Este fenómeno es conocido como *glocalización*, que hace referencia a la importancia ganada por lo local en escenarios globales, a partir de valerse de las mismas herramientas tecnológicas para posicionar los temas endógenos en la agenda. Así, el factor cultural se evidencia en esta revolución, pues son en definitiva los elementos culturales los que permiten que las aplicaciones tecnológicas tengan éxito y sentido (Fernández, 2018), en la medida que sean efectivos para comunicar y solucionar los problemas que aquejan a las sociedades pluriculturales y pluriétnicas.

La cuarta revolución ha provocado tan profundas transformaciones en la vida del ser humano en las últimas décadas que ha llegado al punto de motivar la acuñación de un nuevo estadio de evolución: el *infolítico* (Matías, 1995). En este estadio se han presentado transcendentales cambios, no tanto cuantitativos como cualitativos, gracias al acceso y manejo adecuado de la información generada a cada instante. No obstante, esta revolución, como todas las anteriores, también posee un lado negativo, encarnado en el determinismo técnico, la preponderancia de lo cuantitativo, la multiplicidad de espacios delictivos (internet profundo), el caos disfuncional e inclusive las brechas tecnológicas y de acceso a la información (Fernández, 2008).

Este nuevo entramado de relaciones humanas pone de manifiesto la estructuración de un nuevo escenario de acción humana, el *ciberespacio.* Esta zona se ha convertido en un nuevo ámbito que, junto con los escenarios tradicionales de presencia humana (tierra, mar, aire y espacio exterior), constituye el entorno donde se desarrollan las actividades económicas, productivas y sociales de las sociedades contemporáneas (Escuela de Altos Estudios de la Defensa, 2014). Por esto, al ser un escenario de relaciones humanas, inevitablemente se originan mecánicas de conflicto entre los distintos grupos o individuos (París, 2013) que buscan garantizar y satisfacer sus propios intereses y necesidades, los cuales son diferentes en cualidades y cantidades.

Al observar la creación de este nuevo espacio de acción humana, el Departamento de Defensa de Estados Unidos fue uno de los primeros organismos gubernamentales en conceptualizar este nuevo territorio de conflicto. Las definiciones son variadas, ya que van desde la aceptación del entorno en donde la información digitalizada se comunica a través de redes informáticas, hasta formas más complejas que tienen en cuenta el dominio caracterizado por el uso de la electrónica y el espectro electromagnético por medio de una red interdependiente de infraestructuras de tecnologías de la información y de la comunicación (TIC) (Singer & Friedman, 2014). Una red de infraestructuras donde se crea, almacena, modifica, intercambia y explora información de manera constante (Ortega, 2012) y que permite el correcto funcionamiento de la estructura critica de las sociedades (Stel, 2014).

En este sentido, se puede decir que el ciberespacio, a diferencia de los dominios humanos anteriores (tierra, mar, aire y espacio exterior), que son de origen natural, es un escenario artificial creado por los humanos y utilizado para su servicio. En consecuencia, se puede entender el ciberespacio como una dimensión donde se desarrollan procesos tanto bélicos como no bélicos, y que es transversal e integra las dimensiones naturales de dominio humano. Esto es posible gracias al incontable número de interconexiones, así como al hecho de que muchas de las herramientas, maquinarias y demás elementos que se utilizan en los espacios naturales dependen de la información generada en el ciberespacio para funcionar (Gaitán, 2018). Bajo esta lógica, el ciberespacio logra trascender límites geopolíticos y socavar las fronteras de los Estados, lo que representa grandes riesgos para la seguridad, defensa y soberanía nacional. Sin embargo, también permite una integración de operaciones de la infraestructura crítica de gobernabilidad, comercio y seguridad nacional (Gorman, 2005).

La configuración del ciberespacio y la naturaleza conflictiva de los humanos da paso a la lógica de la guerra en el espacio cibernético, donde existen riesgos y amenazas para las personas, los Estados, las empresas y grupos sociales en general. *The Economist* (2010) definió el ciberespacio como el quinto dominio de batalla, concepto que fue aceptado y avalado por la Organización del Tratado del Atlántico Norte (OTAN, 2016), como un dominio militar legítimo para desencadenar acciones de protección militares conjuntas y coordinadas entre las instituciones públicas y privadas.

Amenazas a la seguridad y defensa en el ciberespacio

Conforme avanza el siglo XXI, los desarrollos tecnológicos atados a internet y al campo de la computación han penetrado todos los aspectos de acción de un Estado. Gracias a estos desarrollos, las autoridades pueden monitorear las redes de servicios públicos esenciales, los sistemas de transporte y de comunicaciones, almacenar información de interés para la seguridad nacional, entre muchas otras acciones estratégicas (Gücüyener, 2017).

Este nuevo escenario ha traído consigo el surgimiento de nuevas amenazas que pueden poner en riesgo el normal funcionamiento del Estado y sus habitantes, ya que la infraestructura del Estado también se ha vuelto más vulnerable a atacantes que se camuflan en la inmensidad de la red. Debido a que brinda un anonimato y dificulta la trazabilidad del delito, la red se ha vuelto muy atractiva para cometer ilícitos (Harknett & Stever, 2011).

Ante este panorama, se ha hecho prioritario que cada Estado, de acuerdo con su contexto, defina un catálogo de su infraestructura crítica[1], teniendo en cuenta que el acoplamiento de esta con internet cada vez es más estrecho. Esto se hace con el objetivo de centrar sobre dicha infraestructura las capacidades de seguridad y defensa cibernética que posea el Estado.

Las amenazas en el espacio cibernético tienen algunas características comunes, entre ellas las siguientes: no se necesitan grandes recursos para cometer ciertos delitos; la posibilidad de anonimato que ofrece internet y la dificultad técnica que requiere rastrear un ataque ha hecho que estas modalidades sean atractivas (Candau, 2010); por lo mismo, no necesariamente debe haber un respaldo estatal para la comisión de actos de cibercrimen, ciberterrorismo, ciberespionaje o *hacktivismo*; y por último, muchas veces la motivación de los grupos que cometen estos crímenes solo es obtener reconocimiento intelectual y no necesariamente obtener ventajas militares o económicas (Carr, 2010; Villanueva, 2015; Weimann, 2005). Estas amenazas pueden ser catalogadas en cuatro grandes grupos: cibercrimen, ciberespionaje, ciberterrorismo y ciberguerra (Burton, 2015).

En el caso del cibercrimen, este está dirigido principalmente a sujetos privados, y se diferencia del espionaje porque rara vez hay Estados patrocinando ese tipo de actividades. En contraste, el ciberespionaje suele estar conducido por agentes estatales o por privados auspiciados por Estados. El objetivo de esta modalidad es robar información sensible con propósitos comerciales, políticos o militares, que le permitan al Estado receptor de la información obtener una ventaja estratégica. De todas las amenazas, esta es quizás la más difícil de detectar y combatir, ya que se diseña para no interrumpir el desarrollo normal de las actividades objeto del monitoreo y por tanto puede pasar desapercibida (Burton, 2015; Rudner, 2013).

Las categorías restantes comparten la característica de que no hay aún un consenso académico acerca de cómo se pueden definir y cuáles son sus características, entre otros aspectos metodológicos. La ciberguerra puede ser entendida como ataques a la infraestructura digital de un Estado en el marco de operaciones militares que pueden comprender otras dimensiones de batalla (Burton, 2015).

1 La infraestructura crítica puede ser definida como la red de activos que son importantes para el buen funcionamiento de la sociedad y la economía de un Estado; por ejemplo, el sistema bancario, el transporte, hidrocarburos, entre otros (Wenjia et al., 2012).

Como última categoría se encuentra el ciberterrorismo, probablemente el mayor desafío para la seguridad de los Estados en la actualidad. Autores como Rudner (2013) lo definen como el uso de información basada en la web para realizar operaciones en el área digital con el fin de crear miedo o violencia, mientras que Marsili (2019) lo entiende como un acto comprometido políticamente y motivado contra sistemas informáticos, programas o datos, a los cuales se ingresa de manera violenta.

El principal blanco de los ciberterroristas es la infraestructura crítica, pues con pequeños golpes se pueden maximizar la sensación de terror y el cubrimiento mediático. En países como Estados Unidos, esta es la amenaza a la que mayor temor le tienen las autoridades, pues existe cierto miedo a una especie de Pearl Harbor digital. Parte de ese miedo ha motivado a las autoridades a actuar y mejorar las capacidades de ciberdefensa (Weimann, 2005).

Rudner (2013) plantea una posición en cierto modo crítica, ya que considera que, si bien el ciberterrorismo es un peligro real para la seguridad estatal, no hay posibilidad de ataques de corte terrorista a la infraestructura cibernética de un país, y por tanto no se puede hablar de ciberterroristas propiamente. De hecho, afirma que no hay evidencia de que grupos terroristas como Al Qaeda o Estado Islámico usen las TIC para acciones terroristas en el campo cibernético. Para él, la problemática está en que grupos terroristas convencionales como los ya mencionados usen plataformas virtuales, como, por ejemplo, las redes sociales para el reclutamiento de potenciales terroristas. De ahí que los Estados deban vigilar esos espacios de posible reclutamiento para evitarlo.

En una posición más crítica a la dimensión general de las amenazas se encuentra Weimann (2005), quien considera que el temor a un Pearl Harbor digital ha sido el gran detonante para que el término se haya hecho famoso. Según Weimann, muchas compañías del sector de la seguridad que subsisten de los recursos estatales destinados para tal fin han explotado ese miedo con fines comerciales. Esto ya que, a juicio del autor, el combate contra el ciberterrorismo no es políticamente rentable aún, pero sí lo es económicamente.

Adicionalmente, muchas acciones que son catalogadas como ciberterroristas en realidad corresponden a hechos de *hacktivismo*. Esta confusión revela que el público y los medios en general desconocen la diferencia y sobreestiman algunas acciones. Para Weimann (2005), la diferencia radica en que el ciberterrorismo puede tener consecuencias serias como la muerte de personas y causar un profundo temor de la sociedad por medio del daño de sistemas informáticos o el simple sabotaje, mientras que, por su parte, el *hacktivismo* se reduce a acciones de protesta que alteran el orden y llaman la atención de los medios; muchas veces estas acciones se limitan a envío de correos masivos, la irrupción en páginas web y la sustitución del contenido original por consignas o el robo de información para hacerla pública.

Pese a que el método más común de los *hacktivistas* es la irrupción en páginas web, muchas veces los medios de comunicación exageran la noticia calificándola de ciberterrorismo, cuando en términos técnicos *hackear* una página es como pintar una pared

con espray (Weimann, 2005). Por esto, se recomienda tomar con cautela los escenarios que impliquen la presencia o intervención de *hackers*, ya que estos suelen exagerar las capacidades de acción de esa comunidad. Solo un porcentaje reducido tiene la capacidad y el conocimiento técnico para realizar ataques masivos a la infraestructura crítica de un Estado.

En todo caso, las ciberamenazas son el gran reto de seguridad de esta época. Por ello la capacidad de inteligencia de los Estados debe estar alerta para poder, en el mejor de los casos, anticiparlas. Debido a la naturaleza reciente y cambiante de las amenazas, y a que tanto el sector privado como el público pueden verse afectados por igual, un imperativo al respecto es cerrar las brechas de conocimiento que existen entre el sector defensa y el sector privado (Manley, 2015). En consecuencia, la gestión y combate de este tipo de peligros debe hacerse de manera conjunta entre los sectores, con el objetivo de que los técnicos desde sus campos de acción compartan conocimientos que permitan refinar la manera de afrontar las amenazas. No obstante, la colaboración entre estos sectores no es fácil y enfrenta dos grandes obstáculos: la falta de confianza y la claridad legal (Manley, 2015).

En cuanto a la confianza, temas como el tratamiento de los datos suministrados por las compañías privadas a los Gobiernos inquieta especialmente, en aspectos como a quién se los pueden compartir los Gobiernos, qué hacen con ellos o si eso puede tener consecuencias adversas para los clientes. Estos temores pueden reducirse si hay claridad legal, es decir, si el Estado provee un marco legal claro y fuerte sobre el tratamiento de datos y los límites que les asigna a los organismos de seguridad (Manley, 2015).

Por otro lado, las capacidades de los Estados en materia de ciberdefensa y ciberseguridad se convirtieron en un tema estratégico de sus planes de seguridad, por lo cual es difícil conocer en detalle las capacidades ofensivas y defensivas que en esta área han desarrollado diferentes actores. Ante esta falta de información, la literatura académica se ha centrado en el estudio de los documentos públicos que emiten los Gobiernos acerca del tema, con lo cual predominan los análisis de las políticas públicas que rodean la creación y dinámicas de las instituciones encargadas de velar por la seguridad y defensa del espacio cibernético.

Los Estados donde mayor interés hay por conocer detalles de las políticas en la materia son Rusia, China y Estados Unidos. En cuanto a Rusia, desde los años noventa empezó a preocuparse por las vulnerabilidades que podía traer la expansión del internet, de modo que sus servicios de seguridad, como el Servicio Federal de Seguridad de la Federación Rusa (FSB), han desplegado arsenales cibernéticos que han sido utilizado en conflictos como Georgia y Chechenia, capaces de generar daño a la infraestructura virtual del adversario. De hecho, ese país es calificado por algunos expertos como el más activo en materia de ciberataques (Carr, 2010).

China hizo lo propio y empezó a prepararse durante la década de los noventa. A finales de esa década, se desplegó el primer ataque de *hackers* de esa nacionalidad —aunque no está claro si estos tenían vínculos con el Gobierno chino— contra las páginas web del

Gobierno estadounidense, tras un ataque accidental a la embajada china en Kosovo por parte de las fuerzas de la OTAN. Sin embargo, es importante destacar que, a diferencia de Rusia, este país es más activo en ciberespionaje (Carr, 2010).

Por su parte, después del 11 de septiembre de 2001, Estados Unidos creó la institucionalidad encargada del control y defensa del espacio cibernético, pero solo hasta 2010 la actuación en este ámbito se declaró prioridad en la agenda de seguridad. En este país, cada fuerza armada posee una división encargada de ese espacio, pero todas son dirigidas por el Comando Estratégico de los Estados Unidos (Usstratcom, por sus siglas en inglés) y por la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) (Carr, 2010; Harknett & Stever, 2011).

De las capacidades de este país se conoce poco, aunque se sabe que de los tres mencionados es el único que ha usado ciberarmamento[2]. Lo hizo en contra del programa nuclear iraní con el gusano *stuxnet*[3], cuyo objetivo era el saboteo de las centrifugadoras encargadas de enriquecer el uranio para posteriormente ser usado en armamento (Burton, 2015; Gücüyener, 2017). Otros países como Irán, Israel y Corea del Norte también son conocidos por emplear ciberataques contra sus enemigos, lo que demuestra que estas capacidades no son del dominio exclusivo de Estados con altos presupuestos de defensa, sino que pueden ser desarrolladas de acuerdo con las necesidades y prioridades de cada país (Carr, 2010; Villanueva, 2015).

En Colombia, el desarrollo de estas capacidades se dio desde 2011 con los Conpes 3701 de 2011 y 3854 de 2016, que trazan los lineamientos en materia de política pública para el desarrollo de las instituciones encargadas de la gestión de la ciberseguridad y ciberdefensa del país, lo cual se aborda más adelante (Villanueva, 2015).

Estructuración de la política en ciberseguridad y ciberdefensa

Relaciones cívico-militares en Colombia

El control de las fuerzas armadas por parte de los Gobiernos democráticos siempre ha sido un tema de interés y debate tanto desde el punto de vista político como académico, debido a que el control permite prevenir la interferencia en política de los militares y asegura la calidad de la institución castrense, especialmente en lo que respecta al monopolio del uso de las armas y al control territorial (Texeira, 2016). En el marco de este debate se articulan las relaciones entre civiles y militares. En todas las democracias del mundo, incluso en las más desarrolladas, es un tema nunca resuelto del todo, ya que constantemente surgen cuestiones de diversa índole que llevan a pensar si el diseño institucional que articula las relaciones cívico-militares es el adecuado o no. Así, estas relaciones están en un

2 Burton emplea el termino *cyber weapons* (Burton, 2015).

3 Oficialmente, el Gobierno de Estados Unidos no ha reconocido su participación en el desarrollo del virus. No obstante, por la complejidad del virus y del ataque, se considera que fue desarrollado entre los servicios de seguridad de ese país e Israel (Burton, 2015).

intrincado equilibrio entre autoridad, influencia e ideología, que debe llevar a los militares a ser una fuerza lo suficientemente fuerte para superar y disuadir amenazas, pero no lo suficiente para convertirse en una amenaza para el régimen donde subsisten (Diamint, 2018; Texeira, 2016).

Igualmente, la injerencia en política de los militares no necesariamente surge dentro de las filas. Recientemente, en países como Venezuela, Bolivia o Brasil, se ha visto una nueva dimensión de la politización de las fuerzas militares que consiste en la cooptación de la fuerza por parte del ejecutivo, con el fin de instrumentalizarlas como pilares del Gobierno. Esto se refleja en acciones como volverlas ejecutoras de las políticas sociales o garantizarle concesiones económicas al complejo militar industrial (Diamint, 2018).

Por esto, el control de los civiles nunca se da como un hecho, sino que se considera un proceso de construcción continua, donde la frontera entre civiles y militares es una delgada línea. Esta frontera se debilita aún más con las nuevas amenazas, por lo cual se hace más necesario ahora definir y mantener el equilibrio descrito (Andrade, 2012).

Esto ha llevado a la academia a estudiar las relaciones cívico-militares, con especial interés en Estados donde las fuerzas militares en algún momento de su historia tuvieron fuertes intervenciones en política, hechos que se evidenciaron como golpes de Estado, y donde las tensiones entre el estamento militar y civil fueron considerables. En este sentido, en el caso de Colombia, quizás por ser un país con la particularidad de que los militares han estado al margen de la política, las referencias al país en los estudios sobre la materia son escasos, y aún más escasos los estudios que se dedican al análisis exclusivo de las relaciones cívico-militares en el país (Schultze-Kraft, 2012).

Samuel Huntington, un autor clásico en la materia, postuló que el control de las relaciones entre civiles y militares se puede categorizar en dos tipos, control subjetivo y control objetivo. En el primer caso, los civiles pretenden dominar a los militares estableciéndoles restricciones legales para reducir su autonomía, inculcando en ellos una conciencia política orientada a la civilidad; por otro lado, el control objetivo se hace por medio de la profesionalización de los militares, con el fin de abrirles nichos de acción que los alejen de la política (Andrade, 2012). Para Huntington, el control de carácter objetivo es el ideal, ya que una fuerza profesional garantiza la independencia de la política. No obstante, ese postulado ha sido ampliamente refutado por diferentes autores que señalan que la profesionalización no es garantía de no injerencia en la política, pues en todo caso los militares pueden hacerlo con el fin de garantizar la supervivencia de la institución o convertirse en guardianes de un régimen en particular (Schultze-Kraft, 2012).

En Colombia, las relaciones cívico-militares podrían ser catalogadas como objetivas, ya que los civiles le apostaron a la profesionalización de la fuerza para garantizar su control y asegurar la no injerencia en política (Andrade, 2012). Sin embargo, el carácter no político de las fuerzas puede también ser explicado por otras razones que van allá de la profesionalización, como el sentimiento antimilitar que tuvo el país durante el siglo XIX y que fue aprovechado por los nacientes partidos políticos para retrasar la profesionaliza-

ción, que se dio solo hasta 1907 —mientras que países como Chile habían iniciado ese proceso en 1830— y evitó la consolidación de unas fuerzas militares que pudieran minar los intereses y el control que tenían los partidos (Andrade, 2012). Incluso la profesionalización fue muy supervisada por las élites políticas, al punto que llevó a convertir al ejército de la primera mitad del siglo XX en un espacio para la burocracia y las elecciones, y no en un ejército encargado de defender las fronteras (Moreno, 2014).

Lo anterior tuvo un primer quiebre con la llegada del Frente Nacional y la denominada doctrina Lleras, con la cual el presidente Alberto Lleras Camargo definió la dinámica de las relaciones cívico-militares que rigen el país hasta la actualidad. Esta doctrina postula la inconveniencia que tiene para el país que los militares participen en política y que los civiles se entrometan en los asuntos de los militares (Andrade, 2012). Esto permitió definir con claridad, por primera vez en la historia del país, las fronteras de los asuntos civiles y militares, y le garantizó al país unas relaciones civiles y militares armónicas en comparación con otros países de la región. Igualmente, el surgimiento de las guerrillas como nueva amenaza a la seguridad interna aceleró rápidamente la separación entre militares y civiles, pues si bien la doctrina le garantizó a los primeros una autonomía en el manejo de sus asuntos, el nuevo contexto llevó a que los civiles les cedieran por completo el control del orden público[4] (Andrade, 2012).

Este hecho es quizás el primer efecto adverso de la doctrina, pues la renuncia por parte de los civiles a la definición de las políticas de seguridad y defensa ha permanecido constantemente hasta la actualidad. Por ejemplo, fuera del Ministerio de Defensa y la Presidencia de la República, no existe un órgano civil encargado de la formulación de las políticas de esta índole, razón por la cual son las mismas fuerzas militares las encargadas de dar los nuevos lineamientos y definir prioridades en materia de seguridad (Schultze-Kraft, 2012).

Esta autonomía permaneció estable durante las décadas siguientes, lo que también puede explicar la subordinación militar hacia los civiles en los años noventa, cuando se dieron algunos intentos por reducir la autonomía del sector, si bien estos no fueron de gran calado. No obstante, se destaca que con el nombramiento de ministros de defensa civiles se intentó aumentar el control civil y democrático al sector (Andrade, 2012).

Un hecho transversal que ha modulado las relaciones cívico-militares en el país ha sido la persistencia del conflicto armado. De hecho, los momentos de mayor tensión entre ambos sectores se han dado en momentos de negociaciones de paz, ya que tales coyunturas abren la posibilidad de renegociar aspectos de las relaciones (Cruz, 2016). De igual forma, la intensificación del conflicto a finales de la década de los noventa y comienzos del nuevo siglo marcó otro hito en las relaciones cívico-militares del país, ya que la decisión de

4 Antes de ese periodo, tradicionalmente los civiles usaban a las fuerzas militares para controlar el orden público en casos de manifestaciones públicas; sin embargo, era un uso esporádico y los militares lo hacían siguiendo órdenes de los civiles. El quiebre radica en que, con el surgimiento de las guerrillas, los militares adquirieron plena autonomía para el control del orden a su discreción (Moreno, 2014).

los gobiernos del momento de aumentar el pie de fuerza y el presupuesto del sector permitió aumentar el grado de influencia que tenían los militares en el sistema institucional. Pero ese cambio solamente fue en el aspecto operativo; en lo doctrinal todo permaneció estable, y la educación castrense continuó con los mismos postulados de la doctrina de la seguridad nacional del enemigo interno (Schultze-Kraft, 2012).

Pero, sin lugar a dudas, este fenómeno se consolidó con la llegada de Álvaro Uribe al poder. Desde ese momento, las fuerzas militares adquirieron una importancia política nunca antes vista en la historia de las relaciones y del país. La razón es que por primera vez hubo una simbiosis entre los intereses políticos y militares, que en este caso era la derrota de la subversión (Schultze-Kraft, 2012). La política de ese gobierno giró alrededor de la derrota de las guerrillas como eje fundamental del desarrollo de las demás políticas de gobierno; por consiguiente, de los resultados militares dependía el éxito de la política de gobierno. Esto ocasionó una subordinación de lo político a lo militar. Para garantizar el éxito militar, los civiles optaron también por aumentar los márgenes de autonomía de la fuerza pública, hecho que ocasionó igualmente un aumento de casos de corrupción, relaciones entre la fuerza pública y actores ilegales, y violaciones de derechos humanos (Cruz, 2016; Schultze-Kraft, 2012).

Durante este periodo, la subordinación de los militares a los civiles estuvo mediada más por la confluencia de intereses que por el control civil (Schultze-Kraft, 2012). Se dio entonces lo que autores como Cruz Rodríguez (2016) y Ramírez (2016) denominan la subordinación desinstitucionalizada, que consiste en que los militares se subordinan a la figura del presidente y no al régimen democrático.

La llegada de Juan Manuel Santos al gobierno ocasionó que el esquema desarrollado durante el gobierno anterior cambiara. En primer lugar, se acabó con la subordinación desinstitucionalizada y se volvió a la subordinación clásica de los militares al régimen democrático; en segundo lugar, se dio un cambio en la forma de abordar la solución del conflicto y se apostó por una salida negociada (Cruz, 2016).

Dado que durante el gobierno anterior los militares habían adquirido una relevancia política sin precedentes, a raíz de las tensiones generadas por el proceso de paz entre el estamento político y militar, se evidenció un intento de un sector de la fuerza pública de interferir en política en acciones como la filtración de información clasificada al expresidente Uribe y la participación en política de algunos miembros, lo que ocasionó su destitución (Cruz, 2016).

Así mismo, por primera vez, la politización de las fuerzas militares fue un hecho de debate y controversia en la esfera política, lo cual llevó a que la cúpula militar solicitara públicamente que no se utilizara a ese sector para hacer política. En medio de los hechos, el entonces presidente Santos, con el fin de asegurar su legitimidad dentro de la esfera militar, aumentó la autonomía del sector.

A partir de lo anterior, se puede evidenciar que actualmente el esquema de subordinación militar está mediado por la confluencia de intereses y el aumento o reducción de la

autonomía militar, más que por un control civil y democrático eficiente hacia los militares o una educación democrática de estos. Por tal razón, se hace necesario que, de cara a la nueva realidad del país, se refuercen y creen mecanismos de control civil y se hagan cambios en la doctrina de educación militar, para enfocarla hacia el respeto por los derechos humanos y el sistema democrático. De igual modo, se deben discutir algunos aspectos de la autonomía militar como el control del gasto, la formulación de la política de seguridad y defensa, entre otros.

Marco institucional

Bajo un contexto de grandes amenazas cibernéticas a la infraestructura crítica del Estado, el MinTIC tomó la iniciativa en la estructuración estratégica de la seguridad de la información, la gestión del riesgo, la resiliencia y la formación de una cultura cibernética, en asocio con el Ministerio de Defensa, el Departamento Nacional de Planeación (DNP) y otras instituciones clave (Contreras, 2019). Este esfuerzo por parte del sector central se materializó en el Conpes 3701 del 14 de julio de 2011, en el cual se establecen los lineamientos para la ciberseguridad y ciberdefensa en Colombia. Con esto, Colombia se convirtió en uno de los primeros países en la región en establecer planes de acciones concretas en la defensa del ciberespacio (Conpes 3854, 2016), puesto que se venía desarrollando una serie de normatividades a nivel nacional y sectorial con incidencia en el tema. Estas medidas van desde el derecho a la intimidad y el buen nombre, pasando por el comercio electrónico, la pornografía infantil, delitos cibernéticos y la regulación del espectro (Conpes 3701, 2011).

El Conpes 3701 tiene como objetivo central "fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio" (p. 20). Para lograr este objetivo se plantearon tres pilares fundamentales:

- La adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.
- El desarrollo de programas de capacitación y formación especializadas en seguridad de la información.
- El fortalecimiento de la legislación nacional y la cooperación internacional en estas materias (Conpes 3701, 2011).

En este documento se le transfiere la responsabilidad al Ministerio de Defensa de abordar de manera efectiva los asuntos de ciberseguridad y ciberdefensa, por medio de la creación, mediante resoluciones posteriores, de órganos técnicos y operativos (Conpes 3701, 2011). Estas nuevas instituciones, que son la máxima instancia de coordinación y

orientación superior en torno a la seguridad digital (Contreras, 2019), están compuestas por una comisión intersectorial que se encarga de plantear la visión estratégica de la gestión de la información y establecer los lineamientos de política en relación con la gestión de la infraestructura tecnológica, la información pública, la ciberseguridad y la ciberdefensa. Está encabezada por el presidente de la República, el alto asesor para la Seguridad Nacional, el ministro de Defensa, el ministro de las Tecnologías de la Información y Comunicaciones, el director del Departamento Administrativo de Seguridad (DAS) o quien haga sus veces[5], el director de Planeación Nacional y el coordinador del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT). Adicionalmente, según las temáticas en discusión, puede invitarse a otros actores nacionales que representen al sector académico, el sector privado, expertos internacionales u otras instituciones del Estado (Conpes, 3701, 2011, pp. 21-22).

Asimismo, se da la creación del ColCERT, que es el organismo coordinador a nivel nacional de aspectos de ciberseguridad y ciberdefensa, en las acciones requeridas para la protección de la infraestructura crítica del Estado. Este organismo presta colaboración a las demás instancias nacionales, como el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC) (Conpes 3701, 2011).

El CCOC es el responsable de la ciberdefensa. Se encuentra bajo la responsabilidad del Comando General de las Fuerzas Militares, que delega funciones dentro de las Fuerzas Militares dependiendo de la especialidad existente en el sector. Su función central es prevenir y neutralizar amenazas o ataques presentes en el ciberespacio que afecten los valores e intereses nacionales, así como la infraestructura crítica del país (Conpes 3701, 2011).

El CCP se encuentra a cargo de la ciberseguridad, por lo cual ofrece a la ciudadanía apoyo, protección y seguimiento ante los delitos cibernéticos, por medio de la prevención, atención, investigación y judicialización. Parte de su deber es informar a través de su página web acerca de vulnerabilidades cibernéticas. Está compuesto por un equipo designado por la Policía Nacional, que debe dar respuesta operativa a los delitos cibernéticos. En su estructura operativa existe un grupo de prevención, uno de gestión de incidentes y otro de investigación, además del Comando de Atención Inmediata Virtual (CAI virtual), que tiene la función de recibir toda la información y reportes de delitos cibernéticos, y la clasificación de las conductas delictivas encontradas en esta dimensión. Asimismo, puede impartir charlas, cursos o visitas para la difusión de temas de ciberseguridad y la prevención de los delitos cibernéticos (Conpes 3701, 2011).

Después de un desarrollo legislativo e institucional desde el Conpes 3701, en 2015 se realizó una evaluación de la política de ciberseguridad y ciberdefensa. Allí se concluyó que el mal manejo de la información y la poca coordinación interinstitucional derivaron en un cruce de información con datos no concluyentes, tanto desde los nuevos órganos

5 Después de la liquidación del DAS en el 2011 por medio del Decreto Ley 4057 de 2011, se creó bajo el Decreto 4179 de 2011 la Dirección Nacional de Inteligencia (DNI), que hace parte de la Comisión Intersectorial.

creados como desde los distintos órganos asesores del sector central y las agencias descentralizadas del Estado en referencia a los alcances del Conpes 3701. No obstante, se resalta que este Conpes 3701 tuvo dos grandes logros: la implementación de la institucionalidad actual en cuanto a ciberseguridad y ciberdefensa, y el posicionamiento de Colombia a nivel regional e internacional como uno de los líderes en la defensa y seguridad en el ciberespacio (Comisión de Regulación de Comunicaciones, 2015; Conpes 3854, 2016).

Con base en un diagnóstico de impacto de la masificación de internet en las actividades socioeconómicas de la población, especialmente en la multiplicación exponencial de los actores individuales y corporativos en el ciberespacio y la economía digital, se identificaron algunas falencias en la política inicial de ciberseguridad y ciberdefensa. Con el propósito de suplir dichas falencias, se creó el Conpes 3854 el 11 de abril de 2016. Este tiene el objetivo de

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (Conpes 3854, 2016, p. 47)

Con esta política, se pasa de un enfoque de política de ciberseguridad y ciberdefensa a un enfoque de seguridad digital. Este Conpes 3854 busca que la sensibilización, la identificación y la gestión adecuada del riesgo, así como las buenas prácticas digitales y la inclusión de múltiples partes interesadas y con responsabilidad compartida —como también las acciones de esta multiplicidad de actores— se enfoquen en maximizar las oportunidades en un entorno digital abierto, seguro y confiable, que contribuya al desarrollo de la economía digital y fomente la prosperidad económica y social (Conpes 3854, 2016).

Para la consecución de este objetivo y para la política de seguridad y defensa en el ciberespacio en general, el Conpes 3854 incluye la gestión del riesgo como eje articulador de los organismos, instituciones y actores presentes en el ciberespacio. Esto surge de las *Recomendaciones de seguridad digital para la prosperidad económica y social* hechas por la OCDE en 2015, como respuesta al continuo incremento del volumen y la sofisticación de la ciberseguridad, derivados del traslado hacia el ciberespacio de las actividades criminales, el terrorismo y las acciones ofensivas y de inteligencia de los Estados. Esto permitió cambiar de un enfoque que busca la preservación de la seguridad de los sistemas de información y las redes, a un enfoque centrado en la gestión del riesgo inherente de las actividades sociales y económicas dentro del entorno digital (Conpes 3854, 2016).

En este sentido, incorpora una perspectiva sobre aspectos técnicos, jurídicos, económicos y sociales, así como contempla los diversos actores involucrados, de forma que promueve la corresponsabilidad en coherencia con los lineamientos de la ONU (Conpes 3854, 2016). Así, la gestión del riesgo en ciberseguridad da la posibilidad de evaluar la

probabilidad de un gran conjunto de posibles ataques, de forma que se pueda determinar la cantidad y la forma de invertir esfuerzos en diseños de protección, medidas de respuesta y recuperación rápida. El proceso de gestión del riesgo requiere la selección entre varias alternativas con diferentes costos y beneficios para reducir el riesgo restante a un nivel aceptable (Castañeda, 2019).

Bajo este marco de gestión del riesgo, se ha identificado que los múltiples grupos y actores que tienen incidencia e interés en la seguridad del ciberespacio y de la infraestructura crítica son los siguientes: el sector Gobierno; el sector defensa; el sector universitario y académico, y el sector mixto y privado (Sánchez, 2019). Esto evidencia que la defensa y seguridad del ciberespacio no concierne de manera exclusiva al Estado y sus fuerzas militares.

En resumen, el Conpes 3701 concentró los esfuerzos del país en contrarrestar el incremento de amenazas en el ciberespacio (Becerra & León, 2019) mediante un marco normativo e institucional para afrontar retos en el entorno digital, estableciendo figuras de enlace y de asesoría sectorial en las entidades de la rama ejecutiva a nivel nacional (Contreras, 2019).

El Conpes 3854 avanzó en el fortalecimiento de las capacidades del Estado y la sociedad frente las amenazas cibernéticas (Becerra & León, 2019). Creó las condiciones para que las múltiples partes interesadas puedan gestionar el riesgo de la seguridad digital en sus actividades socioeconómicas y generen la confianza en el uso de escenarios cibernéticos, por medio de la permanente adecuación del marco legal y regulatorio, así como la capacitación constante de la responsabilidad en el ciberespacio. De esta forma, es un documento que ha fortalecido la dinámica de protección del ciberespacio y de la infraestructura crítica del Estado.

Bajo este contexto, la fuerza pública se planteó en un primer momento alcanzar la supremacía en el ciberespacio, fundamentada en su resiliencia frente a las amenazas (Comando General Fuerzas Militares de Colombia, 2015; Policía Nacional de Colombia, 2015). En este caso se entiende la resiliencia como la capacidad de mantener la seguridad por medio de la flexibilidad y pronta recuperación frente a una serie de posibles eventos adversos, lo que permite la constante revisión de los sistemas y su mejora continua (Castañeda, 2019). Sin embargo, después del Conpes 3854 de 2016, se revisó esto y se vinculó a la gestión del riesgo, en busca de desarrollar estrategias de cooperación con organismos e instituciones responsables del mantenimiento y gestión del ciberespacio, en pro de que tanto entes públicos como privados trabajaran en ello de forma articulada (Comando Conjunto Cibernético, 2017; Ministerio de Defensa, 2016).

Conclusiones

La definición de la política de ciberseguridad y ciberdefensa en Colombia constituye un interesante punto de análisis en el marco de las relaciones cívico-militares en el país, dado

que tradicionalmente fueron las fuerzas militares, en su espacio de autonomía, las encargadas de definir las prioridades y lineamientos en materia de seguridad y defensa. Esa autonomía debe ser redefinida en atención al contexto actual de surgimiento de nuevas amenazas y de necesidad de una política de ciberdefensa y ciberseguridad del Estado. Es en esta política donde se observa un intento de redefinir las relaciones cívico-militares, ya que los civiles se han involucrado más en la definición de prioridades al respecto.

Así mismo, esta política evidencia un cumplimiento constitucional en su definición de funciones entre las Fuerzas Militares y la Policía, ya que las primeras se encargan de la ciberdefensa y las últimas de la ciberseguridad. En el marco de un posible replanteamiento de las relaciones cívico-militares, será necesario abordar estas fronteras; pero en esta política en particular se aprecia un avance en la materia, al menos desde el punto de vista normativo.

No obstante, en la fase de implementación de la política pública, los amplios márgenes de autonomía de las fuerzas militares y el aparente desinterés de las élites políticas se reafirman como en el esquema tradicional, ya que la institucionalidad en el tema está mayoritariamente compuesta por delegados de las Fuerzas Armadas y el papel de los civiles (academia, sector privado, entre otros) es menor. En todo caso, puede surgir de allí un interesante debate sobre la necesidad de un mayor control democrático por parte del sector civil a las capacidades de ciberdefensa y ciberseguridad. Se trata de un debate que puede derivar en la discusión acerca de las relaciones cívico-militares en general.

En todo caso, el desarrollo normativo de la política de ciberseguridad y ciberdefensa, en cabeza de los Conpes 3701 y 3854, demuestra que la materia el país ha emprendido una labor de complementariedad de los documentos en la materia, que tiene como intención robustecer y mejorar las capacidades al respecto. En este escenario cibernético, la gestión del riesgo en seguridad digital no debe ser de la fuerza pública de forma exclusiva ni excluyente. Esta política refleja y plantea la necesidad de integrar una multiplicidad de actores para hacer frente a las ciberamenazas existentes.

Además del contexto mundial del acelerado avance de la cuarta revolución industrial y las crecientes amenazas en el ciberespacio, Colombia se encontraba inmersa en un conflicto armado interno, por lo cual siempre ha existido la necesidad de que confluyan los intereses de todos los sectores del país para actuar mancomunadamente en la protección de la infraestructura crítica física y ahora virtual del país. Por ello, para la seguridad digital, el sector defensa ha estado asesorado y acompañado de manera intersectorial para la gestión del riesgo por otros ministerios y organizaciones civiles.

Agradecimientos

Los autores desean agradecer a la Universidad Militar Nueva Granada por su apoyo en la realización de este artículo.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo. Este es producto de un proyecto de investigación, código INV-EES-2975, titulado "El panorama del postconflicto en Colombia: un acercamiento desde la gobernanza y la reforma del sector seguridad", financiado por la Universidad Militar Nueva Granada.

Financiamiento

Los autores declaran la Universidad Militar Nueva Granada como fuente de financiamiento para la realización de este artículo.

Sobre los autores

Ximena Andrea Cujabante Villamil es politóloga de la Pontificia Universidad Javeriana, especialista en negociación y relaciones internacionales, magíster en asuntos internacionales y doctora en estudios políticos. Docente de tiempo completo de la Facultad de Relaciones Internacionales, Estrategia y Seguridad de la Universidad Militar Nueva Granada.
https://orcid.org/0000-0002-5473-163X - Contacto: ximena.cujabante@unimilitar.edu.co

Martha Lucía Bahamón Jara es abogada de la Universidad Libre, especialista en derecho administrativo y magíster en defensa de los derechos humanos y del Derecho Internacional Humanitario ante organismos, cortes y tribunales internacionales. Docente de tiempo completo de la Universidad Militar Nueva Granada e investigadora adscrita al Grupo de Investigación Sociedad, Estrategia y Seguridad.
https://orcid.org/0000-0002-5877-6886 - Contacto: martha.bahamon@unimilitar.edu.co

Jair Camilo Prieto Venegas es profesional en relaciones internacionales y estudios políticos de la Universidad Militar Nueva Granada y es asistente de investigación en la misma universidad.
https://orcid.org/0000-0002-5894-443X - Contacto: u0901636@unimilitar.edu.co

Jorge Alejandro Quiroga Aguilar es profesional en relaciones internacionales y estudios políticos de la Universidad Militar Nueva Granada y joven investigador en la misma universidad.
https://orcid.org/0000-0002-9494-7574 - Contacto: u0901898@unimilitar.edu.co

Referencias

Andrade, O. D. (2012). Relaciones cívico-militares en Colombia: apuntes para un estado del arte. *Revista Análisis Internacional, 6*. https://bit.ly/2JhePeI

Becerra, J., & León, I. (2019). La seguridad digital en el entorno de la Fuerza Pública. Diagnósticos y amenazas desde la gestión del riesgo. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para*

Colombia (pp. 61-112). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.02

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies, 15*(4), 297-319. https://doi.org/10.1080/14702436.2015.1108108

Candau, J. (2010). Estrategias nacionales de ciberseguridad. Ciberterrorismo. En *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio* (pp. 259-322). Ministerio de Defensa. https://bit.ly/3dvHjze

Carr, J. (2010). *Inside cyber warfare*. O'Reilly Media.

Castañeda, C. (2019). La ciberseguridad, gestión del riesgo y la resilencia, perspectiva de la evolución de la política pública colombiana. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 17-25). Escuela Superior de Guerra "General Rafael Reyes Prieto".

Comando Conjunto Cibernético. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia*. https://bit.ly/2UIsMYy

Comando General Fuerzas Militares de Colombia. (2015). *Plan Estratégico Militar —PEM 2030—*. https://bit.ly/2UEhzbc

Comisión de Regulación de Comunicaciones. (2015, julio). *Identificación de las posibles acciones regulatorias en materia de Ciberseguridad*. https://bit.ly/33L10yB

Conpes 3701. (2011, 14 de julio). *Lineamientos de Política para la Ciberseguridad y Ciberdefensa*. Departamento Nacional de Planeación. https://bit.ly/2UhnzYC

Conpes 3854. (2016, 11 de abril). *Política Nacional de Seguridad Digital*. Departamento Nacional de Planeación. https://bit.ly/3brazVR

Contreras, A. (2019). Gestión de riesgo en seguridad digital en el sector privado y mixto - contexto general. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 169-199). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.05

Cruz, E. (2016). Relaciones cívico-militares, negociaciones de paz y postconflicto en Colombia. *Criterio Jurídico Garantista, 8*(13), 12-41. https://doi.org/10.26564/21453381.581

Diamint, R. (2018). ¿Quién custodia a los custodios?: democracia y uso de la fuerza en América Latina. *Nueva Sociedad, 278*, 24.

Escuela de Altos Estudios de la Defensa. (2014). *Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio.* Ministerio de Defensa de España, Secretaría General Técnica. https://bit.ly/2xloBcZ

Fernández, J. J. (2008). Derechos fundamentales, internet y construcción de la seguridad futura. En J. J. Fernández, J. Jordán, & D. Sansó-Rubert (Eds.), *Seguridad y defensa hoy: construyendo el futuro* (1.ª ed., pp. 15-28). Plaza y Valdés Editores. https://bit.ly/2UkhhYg

Fernández, J. J. (2018). La hiperglobalización y su impacto. *Cuadernos de estrategia, 199*, 83-118. https://dialnet.unirioja.es/servlet/articulo?codigo=6831584

Gaitán, A. (2018). *Ciberguerra. La consolidación de un nuevo poder en las relaciones internacionales contemporáneas*. Ediciones USTA.

Gorman, S. P. (2005). *Networks, security and complexity: The role of public policy in critical infrastructure protection*. Edward Elgar Publishing Limited.

Gücüyener, A. (2017). Understanding the vulnerabilities of critical energy infrastructure to cyber terrorism and threats: How to secure our energy systems. *Strategic Cyber Defense, 48*, 74-85. https://doi.org/10.3233/978-1-61499-771-9-74

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review, 71*(3), 455-460.

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security, 8*(3), 85-98. http://dx.doi.org/10.5038/1944-0472.8.3S.1478

Marsili, M. (2019). The war on cyberterrorism. *Democracy and Security, 15*(2), 172-199. https://doi.org/10.1080/17419166.2018.1496826

Matías, G. (1995). Telecomunicaciones en el umbral del infolítico: una introducción prospectiva. *Situación: Revista de Coyuntura Económica, 1*, 11-21.

Ministerio de Defensa. (2016). *Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2016-2018*. https://bit.ly/39q6IqY

Moreno, J. D. (2014). Relaciones cívico-militares en Colombia: supremacía y control de los partidos políticos sobre la organización militar. *Revista Científica General José María Córdova, 12*(13), 333-352. http://www.scielo.org.co/pdf/recig/v12n13/v12n13a13.pdf

Observatorio de Educación Superior de Medellín. (2019). *Medellín hacia la cuarta revolución industrial. Boletín 11*. https://bit.ly/2UEkpgm

Ortega, L. F. (2012). La ciberseguridad y la ciberdefensa. En *El ciberespacio. Nuevo escenario de confrontación* (pp. 37-69). Ministerio de Defensa de España, Secretaría General Técnica. https://dialnet.unirioja.es/servlet/articulo?codigo=4540377

OTAN. (2016, 8 de julio). *Cyber Defence Pledge* [comunicado de prensa]. https://bit.ly/2wGi2Sa

París, S. (2013). Naturaleza humana y conflicto: un estudio desde la filosofía para la paz. *Eikasia. Revista de Filosofía, 50*(2), 109-116. http://www.revistadefilosofia.org/50-09.pdf

Policía Nacional de Colombia. (2015). *Plan Estratégico Institucional Comunidades Seguras y en Paz. Visión 2030*. https://bit.ly/3dzTFGK

Ramírez C., E. J. (2016). Fuerza Pública, negociaciones de paz y posacuerdo en Colombia. *Análisis Político, 29*(87), 146-149. https://doi.org/10.15446/anpol.v29n87.60757

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence, 26*(3), 453-481. https://doi.org/10.1080/08850607.2013.780552

Sánchez, M. E. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. En G. Medina (Ed.), *La seguridad en el ciberespacio: un desafío para Colombia* (pp. 27-59). Escuela Superior de Guerra "General Rafael Reyes Prieto". https://doi.org/10.25062/9789585216549.01

Schultze-Kraft, M. (2012). La cuestión militar en Colombia: la fuerza pública y los retos de la construcción de paz. En A. Rettberg (Ed.), *Construcción de paz en Colombia* (pp. 405-436). Universidad de los Andes. https://doi.org/10.7440/2012.36

Schwab, K. (2015, 12 de diciembre). The fourth industrial revolution. What it means and how to respond. *Foreign Affairs*. https://fam.ag/3dxPFqb

Schwab, K. (2016). *La cuarta revolución industrial* (1.ª ed.). Penguin Random House Group.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Stel, E. (2014). *Seguridad y defensa del ciberespacio* (1.ª ed.). Dunken.

Texeira, E. G. (2016). Las relaciones entre civiles y militares en la contemporaneidad, un análisis doctrinal sobre el tema. En *Las Fuerzas Militares en los Estados contemporáneos* (pp. 36-49). Pontificia Universidad Javeriana.

The Economist. (2010, 1.º de julio). *Cyberwar. War in the fifth domain*. Briefing. https://econ.st/2UFdDHc

Villanueva, J. C. (2015). *La ciberdefensa en Colombia*. Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00002646.pdf

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict and Terrorism, 28*(2), 129-149. https://doi.org/10.1080/10576100590905110

Wenjia, L., Kodeswaran, P., Jagtap, P., Joshi, A., & Finin, T. (2012). Managing and securing critical infrastructure – A semantic policy and trust-driven approach. En S. Das, K. Kant, & N. Zhang (Eds.), *Handbook on securing cyber-physical critical infrastructure* (pp. 551-571). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-415815-3.00031-5