Los cambios tecnológicos y su impacto en las estrategias de seguridad y defensa

DOI: https://doi.org/10.25062/9786287602489.06

Diego Vera[*],
Paula Prieto[**],
Daniela Garzón[***]

Introducción

Las armas y sus tecnologías cambiantes no explican por sí solas la detonación de conflictos armados y tampoco la trayectoria y desenlace de esos fenómenos. Sin embargo, adquieren enorme relevancia en la planeación de la actividad militar y la formulación de las políticas y estrategias de seguridad y defensa orientadas por capacidades. Máxime teniendo en cuenta la llamada cuarta revolución industrial, que impulsa la convergencia de tecnologías digitales, físicas y biológicas hacia la generación de sistemas complejos y automatizados de diseño y producción en todos los ámbitos, tanto civiles como militares. Una revolución que también

* Politólogo bogotano con énfasis en Relaciones Internacionales de la Pontificia Universidad Javeriana de Bogotá. Magíster en Estudios Políticos e Internacionales de la Universidad del Rosario (Bogotá). Profesor asistente del Departamento de Relaciones Internacionales de la Universidad Javeriana (Bogotá). Investigador y coautor para varios proyectos de la Universidad Javeriana, la Fundación Friedrich Ebert en Colombia (FESCOL) y la Fundación Konrad Adenauer (KAS). Contacto: verad@javeriana.edu.co.

** Politóloga de la Pontificia Universidad Javeriana de Bogotá, magíster en Relaciones Internacionales de la Universidad de Essex (Reino Unido). Actualmente se desempeña como profesional de apoyo a la gestión de investigación del programa de Maestría en Ciencias Militares Aeronáuticas de la Escuela de Postgrados de la Fuerza Aérea Colombiana y es miembro de la Red de Seguridad Ambiental de la Fundación Konrad Adenauer en Colombia (KAS). Contacto: paulaprietoararat@gmail.com y paula.prieto@epfac.edu.co.

*** Internacionalista con énfasis en Estados Unidos-Europa y comunicadora social organizacional de la Pontificia Universidad Javeriana de Bogotá. Investigadora con experiencia en la publicación de artículos sobre temas de relaciones internacionales, seguridad ambiental, política exterior y construcción de paz. Actualmente hace parte de la Red Latinoamericana de Seguridad Ambiental del Programa Regional de Seguridad Energética y Cambio Climático (EKLA) de la Fundación Konrad Adenauer (KAS). Contacto: danny7981@gmail.com.

induce una transformación radical de los asuntos militares y del análisis de la seguridad nacional e internacional.

Precisamente en el avance tecnológico sin precedentes que se está experimentando durante el siglo XXI, destaca la iniciativa de innovación e inversión de los actores privados y la descentralización asimétrica del conocimiento. Si bien tienden a beneficiarse más las sociedades del centro del sistema internacional, de allí surgen activos cognitivos y físicos arduos de monopolizar de forma permanente en un mundo altamente interdependiente e interconectado; sobre todo por la internacionalización creciente de los hallazgos científicos, la multiplicación de canales de difusión de información –incluso reservada– y la apertura hacia diversas oportunidades de comercialización de bienes y tercerización de servicios u *outsourcing*, tanto en los límites de las regulaciones nacionales e internacionales como fuera de ellas.

En un sistema internacional en transición hacia la multipolaridad se configura un nuevo y muy inestable panorama geopolítico con la redistribución del poder económico, político, militar y hasta cultural, no solo entre Estados sino particularmente entre actores estatales y no estatales. Actualmente, parecen converger amenazas y factores de inestabilidad heredados de la Guerra Fría o sistema bipolar, como la carrera nuclear militar, con las fracturas propias de un mundo policéntrico y donde no resulta clara la frontera o matriz ideológica o religiosa principal de los conflictos nacionales e internacionales.

En los conflictos híbridos del presente, se incorporan dinámicas terroristas de múltiples tipologías, mercados ilícitos transnacionales convergentes, actividades disruptivas ocultas en las redes físicas y virtuales, el uso de *proxies* en los teatros de operaciones para eludir responsabilidades directas, y distorsiones en la información por parte de los gobiernos y otros jugadores para desestabilizar o interferir en otros países, además del recurso en aumento hacia medios no convencionales e irregulares de agresión por parte de actores estatales y no estatales para reducir la capacidad de reacción del oponente.

En este sistema en ebullición, el uso dual de estas nuevas tecnologías, tanto civil como militar, económico y político, legal e ilegal, nacional e internacional, complejiza y desafía el pensamiento estratégico tradicional, de modo que expone brechas e interrogantes muy graves para la seguridad y la defensa de los Estados. En definitiva, parecen avanzar más rápido estos nuevos medios bélicos y de enriquecimiento e influencia que las normas domésticas e internacionales para encauzarlos, la cooperación internacional multilateral para desarrollarlos equitativa y pacíficamente, y la reflexión y el consenso académicos sobre sus riesgos y potencialidades.

La presencia de nuevos campos y dominios de la guerra, como el cibernético, obliga a repensar la seguridad y la defensa, así como la reactivación de la competencia espacial y nuclear entre potencias con apoyo de empresas tecnológicas privadas, la instrumentalización

del campo cultural a través de las redes y los movimientos sociales para desafiar las narrativas que dan asiento a la memoria histórica compartida, la verdad jurídica, la autoridad política y los pilares sociológicos de cohesión nacional y, por supuesto, la expansión de las aplicaciones militares con inteligencia artificial y el desdibujamiento de la frontera entre hombre y máquina con la biotecnología. Estos elementos también ponen en entredicho el concepto mismo de la guerra como actividad humana de violencia organizada en función de objetivos político-ideológicos más o menos racionales y que transcurre en un plano físico o geográfico concreto, con operaciones militares por parte de actores armados fácilmente identificables.

En este capítulo se procura trabajar la siguiente pregunta: ¿qué impactos están teniendo las nuevas tecnologías en las estrategias de seguridad y defensa de los Estados en el siglo XXI? Se propone exponer un panorama general, con algunos ejemplos de nuevas tecnologías militares o de potencial uso militar (en prueba) y países que las desarrollan y/o adquieren a partir de la información pública gubernamental, periodística y académica revisada, de forma eminentemente descriptivo-analítica y cualitativa, como estudio de caso exploratorio. Se abordarán los siguientes segmentos: a) un breve marco de referencia sobre las revoluciones tecnológicas, las revoluciones militares (RMA) y las estrategias de defensa; b) la inteligencia artificial (IA); c) el desarrollo espacial; d) los misiles hipersónicos y la disuasión nuclear; y e) la biotecnología y el sector militar. Finalmente, se plantean unas conclusiones y recomendaciones con énfasis en Colombia. Se discutirá el impacto del fenómeno en relación con cuatro estrategias de defensa: disuasión, denegación, interferencia y castigo.

Marco de referencia: revoluciones tecnológicas y militares y estrategias de defensa

El mundo moderno ha transitado por cuatro transformaciones tecnológicas que alteraron profundamente la relación de la humanidad con su entorno y consigo misma, no solamente los modos y medios de producción económica. Los parámetros de organización social y política también cambiaron, incluyendo la forma de conducir las guerras. La primera revolución modificó el patrón de trabajo agrario y artesanal al traer el predominio de la industria y las manufacturas elaboradas por máquinas de vapor, entre 1760 y 1830. La segunda revolución permitió la producción en masa gracias a la generación de electricidad, alrededor de 1850. La tercera revolución facilitó la producción parcialmente automatizada con las tecnologías de la información y la electrónica o computacionales, a mediados del siglo XX (Perasso, 12 de octubre de 2016). Actualmente, la cuarta fase implica la creación y el uso de sistemas ciberfísicos hacia la total automatización, combinando maquinaria física con procesos digitales para hacerlos capaces de tomar decisiones y de cooperar –entre ellos y con los humanos– mediante el internet de las cosas (Perasso, 12 de octubre de 2016).

La cuarta revolución está propiciando cambios en los patrones de evolución del conocimiento, dinámicas de enriquecimiento y relaciones de poder en todas las esferas, y así beneficia a los que más rápidamente se adaptan a y apropian de estas tecnologías (Min, David y Suk, 2018). Esta etapa se caracteriza por la expansión de las industrias de alta tecnología, tanto megacorporaciones como empresas emergentes o *startups*, el uso de medios de transporte eléctrico y ultrarrápido, la investigación y el uso de 'energías verdes' y la comercialización de bienes y servicios derivados del internet, la industria aeroespacial, la impresión en 3D, la ingeniería genética y la computación de generación reciente, como la de tipo cuántico. Aunque varios de estos sectores se basan en los alcances de las tecnologías de la tercera revolución, la nueva característica es la integración acelerada de tecnologías diferentes y que desdibuja las fronteras entre las esferas física, digital y biológica (Min, David y Suk, 2018). Su evolución puede ser exponencial por la velocidad, el alcance y el impacto de esas tecnologías emergentes.

Esta revolución también está incidiendo en el carácter cambiante de la guerra, en la prospectiva de las amenazas y en la revisión de los supuestos del pensamiento estratégico militar. La convergencia de tecnologías informáticas y biológicas hace parte de un nuevo entorno estratégico junto con la geopolítica cambiante, las transformaciones en el mercado global del trabajo, las presiones demográficas contemporáneas y las nuevas aproximaciones y conceptualizaciones de la seguridad (Ryan, 31 de octubre de 2018). En el campo militar, esta revolución puede observarse en el desarrollo de cabezas explosivas más pequeñas, cabezas nucleares tácticas, drones de doble propósito, aplicaciones específicas de inteligencia artificial para operaciones militares y sistemas de armas o la impresión 3D de armas, vehículos y equipos militares, todo lo cual permite elevar la letalidad, precisión, indetectabilidad y producción en masa, al tiempo que se reducen costos y operaciones industriales (Hammes, 24 de agosto de 2018). Pero este escenario no solamente está modificando los medios de la guerra, sino igualmente desatando una nueva revolución en los asuntos militares, ejerciendo influencia sobre cambios en la doctrina, la organización y los procesos de reclutamiento, formación, tácticas y comando de las fuerzas militares en diversos países (Ryan, 31 de octubre de 2018).

En ese sentido, entre finales de los años noventa y principios de los dos mil ya se había advertido en el establecimiento militar de EE. UU. el advenimiento de una "revolución en asuntos militares" (*Revolution in Military Affairs* o RMA), entendida como una transformación inminente en la conducción de la guerra por causa de las nuevas tecnologías, entre las que se destacan las municiones guiadas por sistemas de precisión y las tecnologías de información y telecomunicación (Bousquet, 2017, p. 1). No obstante, las RMA no son un fenómeno nuevo. Los avances en la tecnología y la estrategia tienden a revolucionar la manera como se combate en la guerra a partir de la transformación de la doctrina militar, el entrenamiento, la organización, el equipamiento, las tácticas, las operaciones y la propia estrategia dentro de nuevos patrones para hacer la guerra (Mallick, 2020). De hecho, su concepto antecedente

es de origen soviético, conocido como *Military Technical Revolution* (MTR), en el cual se concibe que ciertos eventos tecnológicos pueden alterar el curso de la historia militar.

Aunque no hay absoluto consenso al respecto, se suele hablar de varias RMA desde el siglo XIV, siguiendo parcialmente a Mallick (2020):

1) La revolución en la infantería (incluso sobre la caballería)
2) La revolución en la artillería
3) La revolución de la navegación y el disparo naval
4) La revolución de fuertes/fortificaciones antiartillería
5) La revolución de la pólvora y las armas de fuego
6) La revolución napoleónica en logística y organización militar
7) La revolución de la guerra terrestre mediante poder de fuego, transportes y comunicaciones
8) La revolución naval con el acero, el hierro y los submarinos
9) La revolución aérea y espacial (aeronaves de combate y telecomunicaciones)
10) La revolución nuclear (bombas y propulsión nucleares)

En la actual RMA, las variables independientes parecen ser innovaciones como las tecnologías para capturar, procesar y distribuir la información, las tecnologías militares en nuevos dominios de la guerra como el espacio, el ciberespacio y hasta el subsuelo, y los dispositivos que permiten mayor maniobrabilidad y más rápidas comunicaciones al personal. Los cambios que están propiciando, como variables dependientes, tienden a ser cuatro: ataques mucho más precisos y a mayor distancia, mejora dramática de los sistemas de comando, control e inteligencia, capacidad para desplegar guerra informática y de información y operaciones no kinésicas ni letales (Mallick, 2020). Sin desconocer estos avances, las nuevas capacidades de las fuerzas militares, incluyendo las de EE. UU., aún no son garantía de superioridad absoluta, particularmente examinando las confrontaciones con insurgencias armadas y actores difusos y resilientes (Bousquet, 2017).

Dentro de ese tipo de cuestionamientos y similares a la actual RMA, subsisten varios interrogantes que hacen que el futuro siga abierto y no sea posible anticipar la forma exacta ni el éxito de esta nueva fase, por ejemplo: a) los elementos políticos e ideológicos, no puramente el cambio tecnológico, determinan su evolución y modo de aplicación militar (Bousquet, 2017); b) el precepto occidental de proyectar poder militar y así reducir la proyección de

vulnerabilidad, usando medios a distancia como los drones, asume que el ajuste técnico permanente basta para acabar con la amenaza (por ejemplo, el terrorismo global), y de este modo ignora sus raíces profundas; c) se podrían estar hiperbolizando las promesas de eficiencia militar del RMA al subestimar la respuesta estratégica de los adversarios, ya que la reducción de riesgo al evitar la exposición directa del personal al combate, operando a distancia, puede ser una invitación a que el enemigo responda con ataques más indiscriminados en contra de su población o infraestructuras para elevar el costo del conflicto y trasladarlo a sus propios territorios "seguros" (p. 17).

Además de los desafíos de los conflictos asimétricos, los interrogantes que surgen de esta nueva fase tecnológica para los propios militares no son menores porque están teniendo impactos directos en los roles del personal e incluso en su alistamiento y formación. Los drones y la inteligencia artificial están dado paso a aeronaves y buques remotamente tripulados y sistemas de armas semi o totalmente automatizados; esto genera presiones de sustitución de funciones, pilotos y operarios, o lo que se conoce de modo más genérico como la 'destrucción de empleos'. Empero, el mundo no parece estar listo económica, social ni psicológicamente aún para dar tan rápido el salto hacia vehículos civiles y militares totalmente controlados por máquinas y programas de computadora (Cukier, 2018). La transición cultural puede acortar el tiempo de implementación, pero también habrá que adaptar los modelos económicos para generar nuevo personal y absorber o recapacitar al remanente laboral, incluyendo los oficiales militares.

Con respecto al campo de batalla, hay una consternación similar por la posibilidad de que los drones y la inteligencia artificial den paso a la producción y al uso de robots de combate o soldados robot en todos los dominios de la guerra, lo que propicia dudas sobre la conveniencia táctica y humanitaria de que ejecuten las misiones, especialmente ante la presencia de civiles. También preocupa que el desplazamiento de la industria militar por parte de las industrias tecnológicas privadas resulte en falta de conocimiento y control de esas armas por parte de decisores políticos y oficiales militares (Cummings, 2018). Sin embargo, también pueden ampliarse las oportunidades de desarrollo profesional para otros oficiales porque los sistemas artificiales de pensamiento requieren de programadores, controladores y supervisores humanos, especialmente cuando las tareas/misiones involucran entornos o teatros muy complejos, donde las habilidades de precisión o detección y las reglas parametrizadas en los modelos no son prenda de garantía para el cumplimiento de los objetivos con el mínimo efecto colateral posible. El razonamiento basado en conocimiento amplio y la experiencia resultan necesarios cuando la incertidumbre es muy alta y se precisa de intuición, buen juicio y rápida interpretación de la situación cambiante, algo difícil de replicar en las máquinas (Cummings, 2018). Por esa razón, la planeación de la guerra en los niveles estratégico, táctico y operacional seguirá siendo eminentemente humana, aunque esté apoyada cada vez más por insumos cibernéticos y su ejecución se lleve a cabo con más medios automatizados.

Como muestras de esta nueva revolución tecnológica en el campo militar, EE. UU. creó su cibercomando en 2010 (USCYBERCOM) y la primera fuerza militar espacial (USSF) del mundo en 2019 y adelanta varios proyectos de integración entre máquinas y organismos biológicos, algunos por cooperación público-privada, encabezados por la agencia gubernamental de proyectos avanzados de defensa (DARPA). Esa agencia señala su misión en el campo biotecnológico: demostrar y generar una transición tecnológica revolucionaria –para EE. UU. y su defensa– a partir de investigaciones, descubrimientos y aplicaciones que logren integrar la biología, la ingeniería, las ciencias computacionales, las matemáticas y las ciencias de la física, incluyendo en su portafolio no solamente innovaciones para la medicina, sino además para desarrollar la interfaz entre humanos y máquinas, usar microorganismos como plataformas de producción, y fomentar la exploración profunda del impacto de las ecologías y los entornos en evolución en la preparación y las capacidades de las Fuerzas Militares de EE. UU. (DARPA, s.f.). Esto ya no es solamente 'doctrina de EE.UU.' sino una realidad pujante en todo el pensamiento militar mundial.

Aunque podría pensarse que son capacidades exclusivas de la superpotencia o de grandes potencias y con pocas posibilidades de reproducción, el mecanismo de emulación entre potencias competidoras, la transferencia de tecnologías a los aliados, y el robo o desvío de información industrial/científica suelen ser mecanismos que inducen la proliferación. Y si bien las potencias en vías de desarrollo tienen enormes dificultades y restricciones para aprovisionarse de estas innovaciones, resultan de uno u otro modo estremecidas por las posibles consecuencias que para su seguridad y la estabilidad mundial tengan esa difusión y esa competencia entre grandes jugadores, lo cual las obliga a actualizarse también en menor proporción o, por lo menos, a responder jurídica y diplomáticamente para compensar su desventaja y mitigar los riesgos y amenazas que perciben de esos avances.

Lamentablemente, el rezago de los civiles, los medios de comunicación y los propios tomadores de decisión (por ejemplo, legisladores y jueces) frente a estos desarrollos puede derivar en situaciones como el debilitamiento del control civil sobre los proyectos de defensa avanzada, la incapacidad de regularlos debidamente en aras del interés nacional (o de la transparencia internacional), la formulación de políticas públicas discontinuas en la materia y hasta la pérdida de oportunidades de investigación, inversión y aplicación relacionadas con estas innovaciones, básicamente por desconocimiento o prejuicios. Sin obviar que las preocupaciones y los límites humanitarios y bioéticos son fundamentales por las fuertes implicaciones en los protocolos de investigación y uso de estas tecnologías, con el agravante de que los regímenes no democráticos que las exploran enfrentan menos restricciones y resultan menos abiertos al escrutinio doméstico e internacional.

En efecto, el principio de rendición de cuentas es central en las democracias. Sin embargo, en asuntos complejos como los sistemas de inteligencia artificial, por su carácter técnico

y la dificultad para explicar su forma de "pensamiento" a las audiencias no especialistas, incluyendo los políticos, la toma de decisiones sobre su desarrollo y uso se hace más opaca (Bryce y Parakilas, 2018, p. 43). Sus aplicaciones militares y posibles consecuencias son tan inquietantes que líderes de la innovación tecnológica como Elon Musk o Mustafa Suleyman enviaron una carta abierta a las Naciones Unidas en 2017 para que se busque una manera de proteger a la sociedad de sus usos indebidos, por ejemplo, con restricciones para los sistemas letales y autónomos de armas (Bryce y Parakilas, 2018).

En otro ejemplo, además de la inconveniencia estratégica de depender crecientemente de infraestructuras, dispositivos y servicios de soporte de empresas de alta tecnología y/o de las inversiones de China en estas áreas, lo cual resta autonomía tecnológica a los países receptores, se viene discutiendo en Europa que ese despliegue, respaldado por el Estado chino, no solamente tiene el objetivo geopolítico de consolidar a China como primera potencia mundial (tecnológica) y así debilitar la influencia de EE. UU. y sus empresas. También se mencionan los peligros del robo de propiedad intelectual e información estratégica y del uso dual de tecnologías digitales para conducir operaciones disruptivas contra sus gobiernos y Fuerzas Militares al permitirle el acceso a sistemas muy sensibles para la seguridad y la defensa, lo que ha llevado a varios países de esa geografía a limitar el monto o los sectores de IED de China (Nelson *et al.*, 2022). Tecnologías emergentes como la inteligencia artificial, los sistemas autónomos, el internet de las cosas y sus componentes, así como las capacidades con soporte espacial, son los blancos de los inversionistas chinos respaldados por su Estado; para el Partido Comunista Chino (PCC), la alta tecnología es el soporte de una economía avanzada, el control gubernamental de la sociedad y unas Fuerzas Militares de capacidad superior, como temas interconectados y orientados por el principio de fusión civil-militar, que facilita el uso dual de todos los avances (Nelson *et al.*, 2022).

Las tecnologías emergentes en conjunción con el despliegue de actores disruptivos y tensiones y rupturas geopolíticas crecientes de un mundo cada vez más multipolar y anárquico invitan a pensar en las repercusiones actuales y futuras para la seguridad multidimensional, la seguridad nacional y la seguridad humana. La complejización de los conflictos armados con nuevas lógicas y actores, o las guerras híbridas y las tecnologías emergentes ofensivas, defensivas y de uso dual (civil-militar), están haciendo más difícil la planeación estratégica en relación con la identificación precisa de las amenazas y de las capacidades y acciones necesarias para contrarrestarlas.

Una forma para aproximarse a las ventanas del cambio estratégico puede ser la discusión del impacto de estas tecnologías emergentes sobre tipos conocidos de estrategias de defensa. A continuación, definimos brevemente cuatro:

1. Disuasión (*deterrence*): es esencialmente psicológica y sucede cuando un Estado usa la amenaza de represalia para imposibilitar una agresión por parte de un

adversario. Su mayor conceptualización se ha dado en el marco de la competencia nuclear armada, donde esas potencias buscan mantener un alto nivel de capacidad destructiva instantánea y abrumadora contra cualquier agresión a ellas o sus aliados. Se basa en dos condiciones básicas: a) la *capacidad* de tomar represalias después de un ataque sorpresa debe percibirse como creíble; y b) la *voluntad* de tomar represalias debe percibirse como una posibilidad, aunque no necesariamente como una certeza (Britannica, s.f.b). Se busca afectar la voluntad estratégica del otro.

2. Denegación (*denial*): es esencialmente material y se usa para dificultar que un oponente logre un objetivo militar. A diferencia de la disuasión, que busca cambiar la intención del otro, la denegación procura poner el objetivo del oponente fuera de su alcance en dos formas: a) cualquier medida para bloquear u obstruir el ataque u ocultar el blanco constituye denegación, ya sea con una barrera natural o artificial (por ejemplo, una muralla); y b) cualquier medida para neutralizar o destruir las capacidades del oponente antes de que realice el ataque (por ejemplo, una zona de exclusión aérea o destruir sus instalaciones militares y sistemas de armas) (Britannica, s.f.a). Se busca afectar la capacidad estratégica del otro.

3. Interferencia: puede ser ejecutada tanto por medios militares como no militares. Se trata de una estrategia disruptiva para manipular o usar los elementos, actores y dinámicas domésticas del rival para obstruir o cambiar el curso de sus procesos de toma de decisión de forma conveniente. Es una estrategia asociada a la guerra híbrida, en la que se utilizan herramientas como la desinformación, la interferencia económica, la interferencia electoral, el apoyo externo a subversión y a sublevaciones o disturbios internos, paramilitares y actores armados no identificados (milicias, terroristas), ciberatacantes (*hackers*, *crackers*, *hacktivistas*) e incluso empresas privadas (Wigell, Mikkola y Juntunen, 2021). Se busca paralizar la toma de decisiones desde adentro.

4. Castigo: involucra el ataque directo a los centros de gravedad o intereses vitales del contrincante como forma de tratar de detener aquellas acciones que se considera afectan los propios intereses nacionales. Puede escalar en términos de intensidad de la respuesta y de tipo de operación militar, empezando con el desarme forzado, la inhabilitación de sus capacidades, repeler con otro ataque y, finalmente, derrotar al enemigo con una ofensiva abrumadora (Kainikara, 2013). Es un tipo de estrategia que en las democracias normalmente se considera de último recurso. Busca causar un daño insoportable o irreparable al enemigo.

Inteligencia artificial

Tradicionalmente se ha visto a EE. UU. con amplia superioridad en investigación y desarrollo de inteligencia artificial (IA), escenario que cambió con la evolución de China y Rusia en la materia. Como reacción a un posible rezago, el país tomó como punto de partida la conformación de un grupo interministerial que analizó el impacto de la IA en la seguridad estadounidense. El resultado fue el informe *Preparing for the Future of Artificial Intelligence* de la Oficina de Ciencia y Tecnología de la Casa Blanca, en el que se reconoce la importancia de la IA como herramienta de transformación en seguridad y defensa. Posteriormente, en 2018, la Estrategia de Defensa Nacional definió la IA como elemento prioritario y vital para la conservación de la ventaja militar (Haney, 2020).

En febrero de 2019, el presidente Trump dio la orden ejecutiva *Maintaining American Leadership in Artificial Intelligence*, que contiene los lineamientos para el fortalecimiento científico, técnico y financiero en investigación y desarrollo en IA y contempla cinco principios esenciales: a) EE. UU. debe dirigir los avances tecnológicos en IA en todo el gobierno federal y la academia para promover el desarrollo científico y económico y la seguridad nacional; b) se compromete con el desarrollo de estándares técnicos adecuados que permitan el desarrollo y testeo seguros de la IA y su acogimiento en la industria; c) procurará la capacitación de las generaciones presentes y futuras en la aplicación de IA; d) fomentará la confianza del público y la confiabilidad de la IA y protegerá las libertades civiles en la aplicación de la IA; y e) promoverá un ambiente internacional que favorezca la investigación e innovación estadounidense en IA y el ingreso de sus industrias de IA a mercados abiertos, para así mantener la protección de su competitividad y sus intereses de seguridad (Haney, 2020).

En esencia, el gobierno estadounidense procura conservar su posición dominante mediante la *Defense Innovation Iniciative, Third Offset Strategy* (Martin, 2019, citado en Romero, 2019). Sin embargo, otros análisis evidencian algunas fallas en la forma como ha tenido lugar la aplicación de la IA en la agenda de seguridad y defensa y que ha afectado la protección de los intereses nacionales estratégicos. Por ejemplo, Almeida (2019) plantea que estas políticas han tenido un campo de acción limitado, principalmente por cuestión de recursos, ya que no se han incrementado sustancialmente. Asimismo, expone la necesidad de que los asuntos relacionados con IA se encuentren regulados por una agencia específica del gobierno, conformada por personal especializado, y dedicada al aval de los sistemas y la creación de estatutos o normas que estandaricen los requerimientos para dichos sistemas.

Comparativamente, cuando el desarrollo de IA de EE. UU. es analizado desde una perspectiva tradicional de capacidad estatal, parece que ha sido superado por China. Sin embargo, al tener en cuenta su sector privado, que ha logrado los mayores avances e innovación –las *startups*–, termina siendo un actor relevante para la adquisición de tecnología a través de las

alianzas público-privadas, incluyendo IA para seguridad y defensa. Así, el panorama apunta a que la superpotencia intenta mantenerse como líder en el área, a pesar de su declive relativo como hegemón global.

Uno de los principales desafíos con el desarrollo de la IA, especialmente cuando no es controlada por el gobierno central, es que estos avances de programación se hacen públicos y pueden desviarse hacia grupos criminales o terroristas que amenacen la seguridad de otros Estados. Es por ello que desde la academia militar se ha recomendado la expansión de las alianzas público-privadas para hacer cumplir los regímenes de propiedad intelectual y reducir la probabilidad del uso malicioso de la IA por parte de actores estatales y no estatales (Chandra, 15 de febrero de 2021).

China, por su parte, ha exhibido sus fines competitivos en IA, pues en gran medida su motivación está alimentada por la percepción del avance estadounidense. Como parte del camino para alcanzar estos fines, China ha destinado grandes presupuestos a planes formulados a largo plazo, políticas y rutas de acción, encaminados a la formación del personal estatal –y militar– en IA (Romero, 2019). El énfasis mostrado por China en asuntos de IA corresponde a un enfoque de innovación, investigación y desarrollo más ambicioso que el desplegado por EE. UU., que está más centrado en la renovación y actualización de tecnologías preexistentes.

Ahora bien, las aplicaciones de la IA en las agendas de China se han dirigido a la estabilidad social interna y la gobernanza internacional, así como a la dominación del mercado tecnológico; incluso el país ha realizado inversiones estratégicas en empresas comerciales de sus competidores. Pese a tener un mayor papel del Estado en IA que EE. UU., la mayor parte de su inversión reciente ha provenido del sector privado, incluyendo elevadas participaciones en industrias estadounidenses. Las inversiones chinas allí ascendieron de 1,5 millones de dólares en 2010, en una sola empresa, a 514 millones de dólares en 25 empresas, en 2019 (Congressional Research Service, s.f., citado en Romero, 2019). Así, la estrategia empleada por China parece favorecer la integración del sector privado y el militar, vinculando capacidades militares en IA.

Precisamente se han presentado conflictos en torno al tema de propiedad intelectual estadounidense, atribuidos a la interferencia de servicios de inteligencia chinos (Romero, 2019). Aparentemente, el gobierno chino realiza constantes monitoreos de la actividad estadounidense en IA desde la institucionalidad y la academia, además de promover la sofisticación de sus propios sistemas y recursos de IA empleados para el hackeo, la filtración de información sensible y el sabotaje de funciones críticas de red (Haney, 2020). Algunas empresas del sector privado estadounidense se abstienen de patentar tecnologías ante los numerosos antecedentes de robo de parte de China y, además, han cuestionado que ningún sistema de *machine learning* reconocido a la fecha ha provenido originalmente de ahí (Haney, 2020).

Una de las maneras en las que el país asiático usa la IA es como herramienta ofensiva psicológica, en la guerra cognitiva, aplicando tácticas como propaganda y desinformación. Se trata del *deep fake*, un tipo de interferencia con IA para generar noticias, videos e imágenes con el fin de engañar al oponente y manipular la opinión pública nacional e internacional (Jing, 28 de diciembre de 2021). China ha mostrado otros avances en implementaciones bélicas y militares de IA, como su uso en sistemas de navegación aérea y reconocimiento de objetivos, y ha logrado exitosamente incorporar estas tecnologías en misiles de crucero de nueva generación.

En cuanto a Rusia, se ha expuesto una actitud de compromiso con el desarrollo de IA, entendiendo su importancia estratégica e instrumental para el Estado. Como consecuencia, ha realizado inversiones en IA aplicada a la protección de información sensible del gobierno, como forma de repeler y contener el acceso a la información y la opinión negativa acerca del régimen del Kremlin (Haney, 2020). Asimismo, Rusia hace uso de IA con fines ofensivos, similares a China, en el marco de la guerra híbrida. Por ejemplo, está el caso de los comicios presidenciales de EE. UU. en 2016, cuando Rusia mostró su capacidad de IA en operaciones de interferencia para manipular el comportamiento electoral. Aunque se perciba como una influencia política externa y no como un ataque a la seguridad, el uso de estas herramientas tecnológicas con fines parecidos es considerado no solo una herramienta de poder blando para persuadir, sino además una vía para debilitar y desprestigiar desde adentro al sistema político y/o el régimen democrático del enemigo (Kamarck, 29 de noviembre de 2018).

El Ejército ruso ha trabajado en el desarrollo de robots controlados mediante sistemas de IA, especialmente en vehículos terrestres y aeronaves autónomas con capacidad de identificación automática de blancos. En marzo de 2018, Rusia publicó planes para la conformación de un Centro Nacional para la Inteligencia Artificial, así como otras iniciativas de defensa, incluyendo la creación de complejos militares dedicados a la aplicación de los avances en IA (Haney, 2020). Por otro lado, ha realizado también algunas transformaciones orgánicas e institucionales en su camino para desarrollar IA, creando la Dirección para la Investigación Científica y las Tecnologías Avanzadas y la Fundación para Estudios Avanzados. Empero, al país se le dificulta lograr mayores resultados en esta materia debido a la falta de financiación (Haney, 2020).

Ahora bien, en cuanto a las cuatro estrategias de defensa aplicadas al tema, la estrategia de disuasión puede verse afectada por el desarrollo de IA, en el sentido en que el cálculo no estaría totalmente inducido por la percepción humana. Como muestra, hoy se programan modelos y algoritmos que arrojan posibles escenarios de confrontación en el Este asiático, incluyendo actores como China, EE. UU., Japón, Corea del Sur y Corea del Norte. En uno, se asume que estos países han invertido en IA a excepción de Corea del Norte y se plantea un panorama en el cual EE. UU. se verá rezagado en el ámbito militar y económico con China, lo

cual ocasionaría que Japón, Corea del Sur y otros aliados de la zona como Taiwán se alineen con la superpotencia para contener a una China en ascenso (Wong *et al.*, 2020).

Después de aplicar el modelo con varias rondas y posibles cursos de acción de cada actor, se llega a varias conclusiones sobre la incidencia de la IA en la estrategia de disuasión. El desarrollo de IA, al ir de la mano con el desarrollo de armas autónomas, hace que los vehículos no tripulados sean menos útiles en dicha estrategia de defensa. En una simulación, la presencia de humanos en una de las plataformas chinas hizo dudar a los oponentes de atacarlas para no escalar el conflicto, a diferencia de otras secuencias en las que no había presencia humana. Al ser la disuasión menos efectiva en ausencia humana, las guerras tenderían a ser más largas a medida que dicho escalamiento del conflicto también se sigue extendiendo (Wong *et al.*, 2020).

Sin embargo, la reducción de riesgo colateral producto del avance de la IA y las armas autónomas, sumado al estatus que produce ser pionero en este tipo de tecnología, hace que sus poseedores lo perciban como un elemento de disuasión. La presencia de la IA en la toma de decisiones tiende a confundir y generar incertidumbre en el oponente por la falta de información sobre estas nuevas herramientas tecnológicas (Wong *et al.*, 2020).

En cuanto al efecto sobre la estrategia de denegación, el avance de la IA permite crear y desarrollar herramientas autónomas que eleven la precisión para identificar y atacar un determinado activo del oponente y de forma más eficiente. Por ejemplo, la IA ayuda a automatizar las tareas de vehículos terrestres y aéreos no tripulados (Dash, 2018). Así, se facilitan los ataques preventivos y a distancia para reducir la posibilidad del oponente de desplegar sus capacidades militares, mediante armas cibernéticas inteligentes y drones.

El desarrollo de la IA también hace que la estrategia de interferencia tome relevancia. En marzo de 2022, se informó sobre la manera como el uso de IA por parte de los bancos en EE. UU. para comercio, aprobación de créditos y funcionamiento de aplicaciones, entre otros, incrementa el riesgo de ciberataques por parte de Rusia, ya que las herramientas de ciberseguridad que usan siguen siendo rudimentarias. Además, la protección viene de agentes privados que imposibilitan tener cifras claras acerca de los incidentes y ataques (Thomas, 23 de marzo de 2022). China y Rusia ya tienen las capacidades y recursos para optar por estrategias de interferencia basadas en IA, incluso Rusia ya ha optado por desplegarlas, retomando el caso de las elecciones de EE. UU. y de países de la Unión Europea donde usó la desinformación.

Frente a la estrategia de castigo, aquí se considera como la que tiene menores beneficios en IA. Primero, porque esta estrategia se usa como último recurso, debido a que, si el atacante no obtiene resultados devastadores –parálisis estratégica–, podría esperarse una respuesta aún más fuerte por parte del agredido y que podría ser convencional o masiva. Segundo, en el contexto actual de la guerra híbrida, el empleo del castigo por medio de la IA conduce a

resultados difusos, ya que en vez de destruir al enemigo o intimidar a la población civil para que presione al gobierno central a la rendición, podría elevar el sentimiento de venganza. El ejemplo son los ciberataques entre Rusia y Ucrania, donde se desdibuja la línea entre ataques a los militares y los civiles, lo cual ha hecho que aumente la participación de cibervoluntarios para la resistencia ucraniana (Elliot, 14 de marzo de 2022).

Desarrollo espacial

Con el nuevo siglo se han empezado a construir rutas estelares y a comercializar el espacio a través de la expansión de la industria (Álvarez Montero, 2021). Durante cincuenta años, gran parte de la visión sociopolítica, económica y militar del sistema internacional se definió por EE. UU. y la URSS y la centralidad de una confrontación nuclear bipolar. Sin embargo, casi tres décadas después, se ha catalogado el periodo como una nueva era espacial, con otros países protagonistas y otros sujetos, como el sector privado en cabeza de empresas como SpaceX y Blue Origin. La presente época ha fomentado un mayor número de actividades en el espacio y esto ha provocado innovaciones y desafíos para la seguridad. Desde 2015, países como China, EE. UU., Irán, Francia y Japón han creado unidades militares independientes para contrarrestar amenazas a sus activos en el espacio (Cabrera-Ortiz y Ospina-Gutiérrez, 2021).

La competencia por la conquista militar del cosmos se desprende de la agenda pública que dominó la era bipolar. Sin la contienda entre el occidente capitalista y el oriente comunista por el desarrollo de armamento estratégico y los programas espaciales militares, hoy no se podría entender el espacio como un teatro con operaciones de fuerzas especiales, ejercicios militares y avances tecnológicos que le dan la vuelta al mundo. La tabla 1 expone los hitos de las dos principales potencias militares espaciales desde la Guerra Fría, así como algunos de sus actuales programas de defensa ultraterrestre.

Tabla 1. Hitos y programas de defensa ultraterrestre de las potencias militares espaciales

País	Programas espaciales
Estados Unidos	1949: creación de un campo de pruebas de misiles balísticos intermedios e intercontinentales en Cabo Cañaveral, Florida, en el marco del Programa Star Wars. 1958: creación de la Administración Nacional de Aeronáutica y del Espacio (NASA), a través de la Ley del Espacio. 1958: impulso a la Oficina de las Naciones Unidas para Asuntos del Espacio Exterior, el primer organismo internacional para la cooperación internacional pacífica en el espacio. Finales de los cincuenta: lanzamiento del proyecto High Frontier. Su objetivo era crear un escudo antimisiles tierra-aire de varias capas que pudiera rastrear, interceptar y destruir misiles balísticos enemigos. Década de los sesenta: lanzamiento del Programa Espacial Apolo, con el que se planteó transportar personas a la Luna. En diciembre de 1968, la misión tripulada Apolo 8 realizó su primer vuelo en órbita lunar y el 20 de julio de 1969, la misión tripulada Apolo 11, realizó su primer alunizaje.

País	Programas espaciales
Estados Unidos	1972: firma del Tratado de Misiles Antibalísticos (ABM o ABMT) que estuvo en vigor desde 1972 hasta 2002 y limitó a las partes a 100 misiles antibalísticos. 1972-1979: conversaciones sobre la Limitación de Armas Estratégicas (SALT) I-II. Después, en 1991, se dio la firma del Tratado de Limitación de Armas Estratégicas (START 1). Los anteriores tuvieron como objetivo prohibir la colocación de armas nucleares o cualquier otro tipo de armamento de destrucción masiva en la órbita terrestre. 1998: la Estación Espacial Internacional fue puesta en órbita. Esto fue resultado de la colaboración de las agencias espaciales de EE. UU., Rusia, Japón, Canadá y Europa. 2017: la NASA lanzó Artemis, un programa internacional que para 2025 pretende reanudar el transporte humano a la Luna y luego ir a Marte. 2018: establecimiento de la Fuerza Militar Espacial de EE. UU. 2021: primera reunión del Consejo Nacional del Espacio (NSC).
Rusia	A diferencia de EE. UU., Rusia delegó las responsabilidades del espacio exclusivamente al sector militar. 1955: el Comité Central del Partido Comunista y el Consejo de Ministros de la URSS establecieron la Instalación Tayga para dar paso al dominio de la investigación científica en el espacio. 1955: creación de la base militar espacial en Kazajistán. El Cosmódromo de Baikonur fue el primer y más grande puerto espacial del mundo. 1959: primer objeto hecho por el hombre en alcanzar la órbita heliocéntrica. El 12 de septiembre de 1959, Luna 2 aterrizó en la Luna y menos de un mes después, Luna 3 tomó sus primeras fotos del lado oscuro del satélite. 1961: lanzamiento de una sonda espacial que midió la atmósfera de Venus. Ese mismo año, Yuri Gagarin se convirtió en la primera persona en viajar al espacio. 1971: la órbita terrestre baja Salyut 1 (DOS-1) fue la primera estación espacial del mundo. Otras siete estaciones fueron lanzadas como parte del programa. Década de los noventa: el colapso del imperio soviético provocó el declive temporal de los programas espaciales rusos. Las Fuerzas Espaciales Rusas se crearon el 10 de agosto de 1992. 1992: creación de la Agencia Espacial Rusa. En 2004 se transformó en la Agencia Espacial Federal (Roscosmos), que se ubica en Moscú y trabaja con el Comando de la Fuerza Aérea ruso. 2003: Rusia forma parte del Proyecto Soyuz en colaboración con la Agencia Espacial Europea. 2011: primer lanzamiento del vehículo Soyuz-ST-B, que se puso en órbita dos de los satélites europeos Galileo. 2021: Roscosmos firmó un memorando de entendimiento con la Administración Nacional del Espacio de China (CNSA) para la construcción de una base permanente en la Luna. También se anunció que para 2024 abandonará el programa de la Estación Espacial Internacional (ISS) y construirá la nueva Estación de Servicio Orbital Ruso en 2025.

Fuente: elaboración de los autores con base en Catrinel (2022).

Además de Rusia y EE. UU., el juego espacial ha estado protagonizado por otras naciones importantes en el desarrollo de programas civiles para la investigación científica, así como proyectos militares dirigidos a los sectores de comunicaciones por satélite y la recopilación de información para inteligencia. El florecimiento de actores como China, India, Israel, Japón, la Unión Europea, Gran Bretaña, Alemania, la Liga Árabe, Sudáfrica y Brasil, entre otros, se

ha traducido en un escenario de dominación global incierto y ha provocado una espiral de armamento espacial. Cabe mencionar los siguientes casos (Catrinel, 2022):

- China: en 2021 se convirtió en el tercer Estado en establecer comunicación con la superficie de Marte, después de Rusia y EE. UU. El 30 de enero de 2022, Xihe-1, el primer satélite de exploración solar de China, fotografió la línea espectral solar H-alfa desde la órbita.

- Israel: es una de las siete potencias espaciales con autonomía en la producción de satélites y vectores de lanzamiento. Su autonomía está garantizada por Shavit, el vehículo de lanzamiento independiente capaz de enviar cargas a la órbita terrestre baja, y por su programa espacial enfocado en la producción y el lanzamiento de telescopios y satélites.

- India: su Agencia de Defensa Espacial fue creada en 2018, con la meta de realizar misiones de recopilación de inteligencia satelital y guerra espacial. En 2019, probó con éxito un arma antisatélite, realizó la Misión Shakti y ejecutó una prueba de arma antisatélite (ASAT). Además, llevó a cabo su primer ejercicio simulado de guerra espacial llamado IndSpaceEx.

- Japón: es la séptima potencia en producción y lanzamiento de satélites espaciales por medio de estrategias de posicionamiento, navegación y temporización. En 2020, estableció el Escuadrón de Operaciones Espaciales dentro de la Fuerza de Defensa Aérea, con sede en la Base Aérea de Fuchu, Tokio.

- Gran Bretaña: en abril de 2021 estableció el Comando Espacial del Reino Unido con el que desarrolló el programa de comunicaciones satelitales militares Skynet, que brinda cobertura a casi todo el mundo.

El creciente número de satélites, operadores y aplicaciones comerciales ha convertido el cosmos en algo tan esencial como el espacio aéreo y el mar. El desarrollo de las capacidades espaciales está vinculado con sus posibles usos militares. Así lo fue en sus inicios con los satélites espía y la tecnología balística de EE. UU. y la URSS, y así lo es hoy con los sistemas de comunicación, observación y posicionamiento. Ahora, los Estados están viviendo la transición de la guerra mecanizada a la guerra informatizada del siglo XXI, donde el campo de batalla se ha ampliado hasta el espacio y la tecnología espacial dirige unidades de combate (Berrío, 2008).

En relación con la seguridad, el espacio se ha consolidado como un área en constante contienda. En este sentido, es preciso ahondar en tres dimensiones relevantes. 1) Geoespacialidad: el espacio debe ser visto como una región más de la Tierra que tiene características operativas, ambientales e infraestructurales que pueden estudiarse como un conjunto o de

manera particular. 2) Legalidad: el espacio exterior, incluyendo la Luna y otros cuerpos celestes, no debería ser sujeto de ninguna reivindicación de soberanía por medio del uso, la ocupación u otros medios de exploración o utilización del espacio; existe un régimen internacional que busca el desarrollo de normas, mecanismos, acuerdos y cooperación que busca regular el comportamiento de los Estados en el espacio exterior y limitar la hegemonía militar para garantizar la paz. 3) Historicidad: el progreso de los medios aerostáticos, aeronáuticos y aeroespaciales ha modificado la relación de la vida en la Tierra con el cosmos y ha transformado las motivaciones de los Estados y fortaleciendo sus habilidades (López, 2010).

Estas tres dimensiones exigen la protección de los sistemas espaciales para prevenir, resistir y sobreponerse a las nuevas amenazas que podrían afectar al planeta Tierra, pero también al control de las redes satelitales estatales que pueden ser blanco de ataques. Los asuntos geoespaciales, legales e históricos enfrentan la espiral del armamento espacial entre los Estados, que buscan protegerse desde todos los frentes. Actualmente el espacio juega un papel en inteligencia de los países, vigilancia y reconocimiento, respuesta a desastres, seguimiento del movimiento de tropas en tierra, mar y aire, telecomunicaciones clasificadas y no clasificadas, seguimiento del movimiento de refugiados, identificación de pruebas de crímenes de guerra, genocidio u otras violaciones de los derechos humanos, operaciones con drones, armas guiadas por GPS y, por supuesto, el fenómeno de la guerra cibernética, ligada a las tecnologías satelitales (Steer, 8 de enero de 2020). A medida que el cosmos se ha militarizado y que las actividades militares en la Tierra dependen más de las tecnologías espaciales, todos los actores continúan creando una escalada parecida a la de la Guerra Fría, pero multipolar, previendo diversas confrontaciones espaciales. Eso plantea una honda preocupación tanto para las grandes potencias que desean la supremacía tecnológica como para los Estados con alta dependencia y que son los más vulnerables (Steer, 8 de enero de 2020).

Ahora bien, con respecto a la relación entre desarrollo espacial y las cuatro estrategias de defensa descritas, se resaltan los siguientes elementos:

Desde la carrera espacial de la Guerra Fría, la tecnología satelital ha sido esencialmente usada en disuasión y monitoreo nuclear y en apoyo –técnico, no kinésico– a las operaciones militares terrestres, marítimas y aéreas, mas no como recurso primario de acción bélica. De hecho, el propósito de las misiones espaciales ha sido la conquista del espacio exterior especialmente como factor de prestigio. Aunque esta carrera espacial se ha extendido hasta la actualidad por medio del surgimiento de nuevos poderes y actores, su carácter esencial continúa siendo de disuasión militar, comunicación e innovación científica, ya que la guerra todavía se entiende y ejecuta en otros dominios. Esto ha provocado que el espacio se convierta en un área de congestión, competitividad y disputa tecnológica, en tensión con la intención de fortalecer el derecho espacial para la conservación de la paz, pero aún no es una zona de guerra, si bien no se puede ignorar que las potencias principales espaciales están probando

el emplazamiento de armas nucleares, láser y otras que podrían lanzarse desde activos en el espacio hacia puntos terrestres específicos.

El armamento espacial que se está investigando podría usarse como una herramienta de denegación. Actualmente, la tecnología espacial militar ha logrado la capacidad de neutralizar o destruir facultades satelitales de los oponentes, así como afectar sus habilidades estratégicas. China desarrolla armas orbitales con aptitud de lanzar proyectiles y armas antisatélite para cegar, bloquear y destruir naves espaciales desde la superficie y en órbita. Rusia ha anunciado su intención de crear una nave espacial llamada Zeus para destruir satélites y naves enemigas a través de pulsos electromagnéticos de alta potencia. A su vez, la Fuerza Espacial de EE. UU. ha manifestado interés por la construcción de armas terrestres (*meadowlands*) capaces de incapacitar satélites adversarios (Díaz, 13 de julio de 2021). Si bien muchos son solamente proyectos, el teatro de guerra espacial tenderá a evolucionar con la creciente voluntad estratégica de innovar para contrarrestar el avance militar de otros.

Igualmente, las armas espaciales podrían usarse en la estrategia de interferencia a gran distancia. En el marco de la guerra híbrida, los satélites pueden usarse como activos para potenciar el hackeo o la desactivación de satélites de otro país, de modo que se afecten su capacidad de comunicarse y los contenidos, aunque hoy se consideran estos actos como *casus belli* o razones legítimas para responder con medios de guerra convencional (*DW*, 2 de marzo de 2022). Pese a que puede resultar muy contraproducente usarla así, no se descarta que la tecnología espacial pueda ser manipulada para fomentar crisis o malentendidos entre potencias, o incluso para afectar los procesos nacionales de toma de decisión y votación desde el espacio ultraterrestre.

Por último, estas armas no son en esencia herramientas de la estrategia de castigo por los siguientes factores ligados al marco regulatorio internacional del espacio exterior. Las fronteras ultraterrestres deben seguir siendo un santuario pacífico donde ningún Estado-Nación puede reclamar soberanía, según el Tratado del Espacio Exterior de 1967. El artículo I establece que el uso del espacio debe llevarse a cabo en beneficio y en interés de todos los países. El artículo III enfatiza que todas las actividades en el espacio deben realizarse de conformidad con el derecho internacional y en el interés de mantener la paz y la seguridad. El Tratado declara que la Luna y todos los demás cuerpos celestes deben ser utilizados con fines exclusivamente pacíficos, aunque es cierto que esto no excluye los usos militares no agresivos, como sistemas de detección de lanzamiento de misiles. Finalmente, la mayoría de los Estados han optado por la promoción del uso sostenible y a largo plazo del espacio a través de la colaboración y la transparencia (Steer, 2017).

Misiles hipersónicos y disuasión nuclear

Los misiles hipersónicos representan una tecnología emergente de elevada preocupación para todos los países por al menos tres razones: a) alteran dramáticamente los cálculos y sistemas convencionales de defensa antibalística y los hacen virtualmente obsoletos; b) en la competencia por su desarrollo, Rusia y China llevan la ventaja sobre EE. UU. y sus aliados, lo que desafía en este componente la unipolaridad y hegemonía militar occidental; y c) las tecnologías para producirlos son extremadamente complejas y costosas, lo que amplía la brecha militar con países en vías de desarrollo. Aún por medio de la venta/transferencia directa, el costo de cada unidad de estos misiles podría ser de entre 89,6 millones de dólares y 106 millones de dólares (Capaccio, 12 de noviembre de 2021), sin mencionar el costo de los sistemas apropiados de lanzamiento y monitoreo.

Sin entrar en los detalles técnicos, en general existen dos tipos de armas supersónicas: los vehículos de desplazamiento hipersónico o HGV (sigla en inglés) y los misiles de crucero hipersónicos, los cuales se caracterizan a continuación, siguiendo a Sayler (20 de julio de 2022):

- En términos de velocidad, pueden superar hasta cinco veces la barrera del sonido (Mach 5 o 6.174 kilómetros por hora).
- A diferencia de los balísticos tradicionales, no siguen una trayectoria parabólica uniforme, de modo que pueden ser maniobrados en el aire hasta su destino.
- Brindan opciones de ataque rápido y a gran distancia contra blancos muy protegidos e incluso móviles.
- Desafían de forma crítica a los sistemas de detección y defensa ya que pueden ser maniobrados a baja altitud, por lo cual hacen casi inservibles los sistemas de radares terrestres.
- La detección retrasada que logran afecta drásticamente el tiempo de respuesta y evaluación de opciones de los tomadores de decisión de los países atacados/atacables, y así propician un único y muy breve instante de interceptación.

Las dos variantes de misiles hipersónicos en prueba y desarrollo son: a) los que usan motores de tipo SCRAMJET o formas avanzadas de turbinas de jet (propulsión de aire), que funcionan de forma idéntica a los misiles de crucero tradicionales, pero volando dentro de la atmósfera y a velocidad superior a Mach 5; y b) los misiles de planeo hipersónico, que pueden

ser vehículos HGV, instalados en cohetes convencionales similares a los misiles balísticos intercontinentales (ICBM, en inglés), que cruzan por encima de la atmósfera y planean a velocidades similares (*Infobae*, 29 de diciembre de 2018).

Mientras EE. UU. ha realizado varias pruebas fallidas a la fecha de finales de 2022, Rusia y China han expuesto públicamente sus avances en la materia. En diciembre de 2018, las Fuerzas Armadas de Rusia lanzaron desde los montes Urales un HGV bautizado Avangard, transportado por un misil balístico. Según fuentes rusas, el aparato avanzó por 6.000 kilómetros sobre la estepa de Siberia y alcanzó la exorbitante velocidad tope de Mach 27 o unos 32.202 kilómetros por hora, para posteriormente golpear un blanco elegido en la península de Kamchatka (Stone, 8 de enero de 2020). Unos meses antes, en agosto de 2018, China lanzó exitosamente el misil de crucero hipersónico Xingkong-2 con motor SCRAMJET, que alcanzó Mach 6 o unos 7.156 kilómetros por hora serpenteando a través de la atmósfera, siendo exhibido supuestamente como uno de los tres tipos de misiles hipersónicos que la República Popular de China alega poseer (Goldberg, 10 de enero de 2020).

Este claro rezago de EE. UU. ha intentado corregirse recientemente elevando el presupuesto en el área y estimulando múltiples programas de investigación, prueba y desarrollo en armas hipersónicas, entre los cuales se destacan: a) para la Armada, el Conventional Prompt Strike y el Offensive Anti-Surface Warfare Increment 2, más conocido como Hypersonic Air-Launched OASuW (HALO); b) para el Ejército, el Long-Range Hypersonic Weapon (LRHW); c) para la Fuerza Aérea, el Air-Launched Rapid Response Weapon (AGM-183) y el Hypersonic Attack Cruise Missile (HACM); y d) dentro de la agencia DARPA, el Tactical Boost Glide (TBG), el Operational Fires (OpFires) y el Hypersonic Air-breathing Weapon Concept follow-on (MoHAWC) (Sayler, 20 de julio de 2022). Complementariamente, el Congreso estadounidense aprobó en 2022 una partida de 550 millones de dólares, de un costo total estimado de 2.500 millones de dólares, para iniciar el despliegue de una constelación de 28 pequeños satélites en la órbita baja terrestre, equipados con sensores infrarrojos, para poder detectar y rastrear los misiles hipersónicos de Rusia y China. Este sistema, llamado Tracking Layer, pretende cobertura global, fue planeado por el Departamento de Defensa y la Agencia de Desarrollo Espacial y adquirió los primeros ocho satélites de las industrias privadas L3Harris y la alianza SpaceX-Leidos en 2020, que serán lanzados en 2023 (Erwin, 15 de marzo de 2022).

Ahora bien, cuando se piensa en esta nueva tecnología, pero dotada de cabezas nucleares, las alarmas son aún más elevadas. En la Guerra Fría se pensaba que la amenaza de retaliación nuclear era la mejor disuasión frente a una amenaza de ataque nuclear (fuego contra fuego), pero hoy esa idea está cambiando. Por una parte, las nuevas tecnologías de sensores para ubicar con mayor facilidad los blancos han generado la idea de que los sistemas de misiles balísticos pueden ser más rápidos, precisos y letales (Futter, 2020). Por otro lado, los

misiles hipersónicos hacen aún más difíciles la defensa antimisiles y la respuesta oportuna al ataque. Sin contar con que la inteligencia artificial y la automatización también pueden aplicarse a esta capacidad nuclear militar. Esa capacidad de ataque nuclear aumentada puede producir el efecto no deseado de nuclearización militar de otros países y esto aceleraría la proliferación mundial (Futter, 2020), ya que incluso si no pueden contar con misiles hipersónicos, el cálculo para los países en inferioridad puede ser que es mejor contar con alguna amenaza nuclear que ninguna para tratar de disminuir la posibilidad de una agresión o, por lo menos, generar la percepción de que alguno de sus sobrevivientes a un ataque nuclear rápido podría desatar una respuesta nuclear, aunque sea retardada.

Las estrategias de disuasión nuclear ya no son tan efectivas por la dificultad para interceptar misiles hipersónicos. La denegación tradicional de poder militar nuclear se hace más difícil por la multipolaridad y la emulación tecnológica (por ejemplo, Irán). Los ataques preventivos kinésicos a recursos físicos o centrales nucleares (por ejemplo, de Israel a Irán) hacen parte de esa denegación desesperada, pero pueden generar respuestas más agresivas (por ejemplo, acelerar la adquisición de una bomba nuclear) o difusas, como el terrorismo. Por estas situaciones, una opinión es que tecnologías tan avanzadas como esa pueden ser disuadidas u obstruidas con estrategias de la llamada guerra híbrida (de interferencia doméstica), a falta de capacidades de emulación (Shea, 20 de abril de 2020). Las capacidades cibernéticas facilitan los ataques ocultos y a distancia y están disponibles para instituciones y actores no militares. El uso de *proxies* permite a los Estados elevar sus estrategias de denegación. La interferencia digital termina siendo una herramienta clave para tratar de hackear los sistemas de mando y control de armas nucleares –y misiles hipersónicos–. Además de demostrar capacidad y voluntad estratégica para disuadir al posible agresor nuclear, pueden ayudar nuevos elementos estratégicos, tales como la conciencia y habilidad del sector privado para implementar estándares de seguridad, la habilidad de los gobiernos para movilizar a los expertos civiles y la capacidad de alistamiento para desatar respuestas firmes, aún si se trata de amenazas no tan inminentes (Shea, 20 de abril de 2020).

Otra clave estratégica para elevar la capacidad de disuasión frente a estas tecnologías es el conocimiento profundo de las doctrinas militares y nucleares de las potencias que las desean o poseen, lo que permite mejorar las anticipaciones o previsiones. En este sentido, doctrinas que se limitan al uso disuasivo podrían confrontarse de otras formas, como la diplomática (por ejemplo, no proliferación y desarme o reducción nuclear mutua). Sin embargo, doctrinas que plantean la posibilidad de usarlas frente a obstrucciones a sus intereses vitales y objetivos estratégicos resultan más agresivas, como sucede actualmente con la publicación de Rusia en 2020 de su política nuclear y las amenazas que ha hecho el presidente Vladimir Putin sobre usar armas nucleares tácticas contra Ucrania en caso de seguir en resistencia armada contra la invasión y anexión de las provincias del oriente, lo que supera el límite entre

superpotencias acordado tácitamente en la Guerra Fría (Castro, 20 de abril de 2022). Aunque allí se requerirían estrategias disuasivas más fuertes, incluyendo la amenaza de retaliación nuclear, la falta de información y las interpretaciones equivocadas acerca de las intenciones del otro pueden ocasionar graves errores de cálculo, con implicaciones más graves que las de la Guerra Fría por el poder destructivo aumentado y la velocidad de esas armas en caso de usar misiles o vehículos hipersónicos como vectores (Castro, 20 de abril de 2020).

En cuanto a la relación entre misiles hipersónicos armados nuclearmente y las estrategias de defensa definidas en el primer segmento, caben varias anotaciones. Las armas nucleares y los nuevos misiles aún son esencialmente usados por su efecto psicológico o disuasivo como amenazas posibles, pero no como recurso primario de acción por su poder de extrema destrucción. Con excepción de las bombas de Hiroshima y Nagasaki lanzadas por EE. UU. contra esas ciudades de Japón en 1945 y que significaron la muerte aterradora de entre 129.000 y 226.000 personas, la mayoría civiles, las armas nucleares no se han utilizado en otro conflicto armado. La velocidad y dificultad de interceptación que le dan estos nuevos misiles a la capacidad de explosión nuclear eleva su efecto psicológico o disuasivo por tenerlas y exponerlas públicamente, tanto contra armas y operaciones militares convencionales como frente a ataques nucleares, pero no necesariamente eleva la posibilidad de uso final, algo que se deriva más de las causas político-ideológicas de las guerras totales que de la tecnología en sí. Tampoco parecen muy útiles para disuadir ataques indirectos o híbridos, como los que caracterizan a las estrategias de interferencia.

Estas armas de destrucción masiva no tienen sentido como herramientas de denegación. Su uso desborda la desactivación o destrucción controlada de las capacidades bélicas del otro y no se pueden usar como escudo contra ataques. Sin embargo, empleados esos misiles con explosivos convencionales, podrían constituir una forma rápida, pero sumamente costosa y con enormes efectos colaterales, de destruir infraestructuras militares, incluyendo donde se sospeche que haya armas nucleares. Más bien, poseer este tipo de tecnologías de vectores para lanzar ataques convencionales o nucleares a mucha distancia incentiva que las potencias que se sienten intimidadas usen diversas estrategias de denegación para obstruir su efectividad (mejorar sistemas de detección temprana de lanzamientos y escudos antimisiles), retrasar su desarrollo o adquisición con ataques a centros de investigación, ingenieros e intermediarios, o destruir directamente las instalaciones donde se encuentran y/o sus sistemas de control. Las ciberarmas pueden ser parte de esa estrategia de denegación para desactivar o alterar los programas de soporte de esos misiles.

Tampoco tienen sentido como parte de la estrategia de interferencia por su uso a distancia y poder de destrucción. Antes bien, su existencia o sospecha de ella en un país puede propiciar que los gobiernos que perciben esa amenaza potencial opten por inmiscuirse en la política interna de aquel para impedir su uso y proliferación desde adentro del sistema político,

mediante múltiples operaciones de desestabilización, desinformación, oposición y distracción. Entre más difíciles de interceptar y evadir sean las armas, más factible es tratar de desactivarlas desde su origen. Aunque se ha discutido el riesgo creciente de la transferencia de armas nucleares a actores no estatales e ilegales, la posibilidad de que adquieran, controlen y usen misiles hipersónicos parece remota por su elevado costo y aspectos técnicos. Sin embargo, hay un riesgo no descartable de que terceros usen ataques cibernéticos para alterar los sistemas de control de estas armas y manipular el conflicto entre potencias, es decir, usando estrategias cibernéticas de interferencia en los sistemas de soporte para crear una crisis con diversos fines, no necesariamente ideológicos (por ejemplo, pedir rescate económico).

Por último, estas armas no son esencialmente una herramienta de la estrategia de castigo por tres razones básicas: a) contra potencias que tienen –o presumiblemente poseen– bombas nucleares, el riesgo de retaliación nuclear es extremadamente alto, ya que algún sobreviviente puede activar esa respuesta; y b) contra rivales muy inferiores y sin esa capacidad, el efecto tan desproporcionado de su uso puede implicar costos financieros, políticos y humanitarios injustificables, incluyendo la retaliación internacional mancomunada; y c) como usualmente los objetivos políticos de la planeación de la guerra son limitados, rara vez buscando la derrota total del enemigo o su aniquilación, el poder aprovechable de esas armas es manipular psicológicamente al rival y elevar la política de prestigio o estatus internacional militar, poder que se pierde totalmente al detonarlas/lanzarlas.

Biotecnología y sector militar

El recurso de las armas biológicas es una práctica antigua en conflictos armados con el propósito de infectar a combatientes, población o cultivos y ganados del enemigo. Los avances en materia de ingeniería genética y sus aplicaciones militares han aumentado la preocupación de la comunidad internacional por los riesgos derivados de posibles guerras bacteriológicas y bioterrorismo (Pérez, 2004). Este tipo de tecnología es de carácter dual, ya que puede destinarse a diversos usos biomédicos civiles y militares o a la fabricación de armas de destrucción masiva.

El manejo de este tipo de armas se ha justificado sobre cuatro puntos fundamentales. En primer lugar, la gran variedad de organismos y toxinas facilita la selección táctica del momento de uso; por ejemplo, podrían ser herramientas para incapacitar temporalmente al adversario o, si se desea, para destruirlo por completo. En segundo lugar, poseen un potencial desmoralizador importante, usando el miedo a una enfermedad o afectaciones a los servicios sanitarios; su carácter imperceptible contribuye en gran medida a que se incentive su efecto psicológico, pues hace imposible prever y organizar la defensa. Tercero, se han considerado como una variante de "armas limpias" o que solo destruyen vidas humanas

y recursos primarios como el ganado y la agricultura, sin afectar la infraestructura o los recursos industriales. Finalmente, son armas baratas en comparación con otras armas de destrucción masiva; sus procesos de fabricación son relativamente sencillos y los Estados pueden mantenerlas ocultas fácilmente. No obstante, los métodos de diseminación son complejos e imprecisos y engloban desde la contaminación directa hasta la propagación mediante proyectiles o la dispersión de aerosoles, polvos o líquidos desde aviones a baja altitud (Alcocer, 2002, pp. 86-87)

A pesar del creciente interés por fortalecer las maniobras biotecnológicas para la guerra, es importante destacar que ha habido pocos ataques biológicos reales, pues la adquisición de los conocimientos y recursos necesarios para la ejecución exitosa de un ataque de esta índole es muy difícil. En la Segunda Guerra Mundial, Gran Bretaña, debido al temor de una invasión alemana, ensayó armas con bacterias de carbunco sobre el despoblado islote de Gruinard –costa noroeste de Escocia–. En los años ochenta, se comprobó que la isla seguía contaminada y que podría permanecer así durante más de un siglo (Alcocer, 2002).

En la guerra de Vietnam, el agente naranja fue un defoliante químico esparcido por aviones y helicópteros de la Fuerza Aérea estadounidense entre 1962 y 1971 para reducir los densos bosques vietnamitas, descubrir los escondites y las rutas de suministro del Vietcong y fumigar las tierras de cultivo para privar al enemigo de alimentos. EE.UU. llevó a cabo más de 6.000 misiones con los distintos defoliantes y se rociaron cerca de 45.677.937 litros de este agente. El contacto con el TCDD (su tóxico activo) provoca lesiones cutáneas, así como daños graves en los órganos, afectaciones en el útero y enfermedades como el cáncer (Freund, 10 de mayo de 2021). Casi tres generaciones después de haber sido usado, muchos niños en Vietnam nacen con graves malformaciones en su cuerpo.

Los primeros esfuerzos internacionales para regular la guerra biológica se dieron a finales del siglo XIX y principios del XX. Con la adopción del Protocolo de 1925, firmado en Ginebra, la comunidad internacional tomó conciencia de la gravedad que plantean los agentes biológicos. Sin embargo, con lo ocurrido durante la Segunda Guerra Mundial y la Guerra Fría, en 1972 se firmó el Convenio sobre la prohibición del desarrollo, la producción y el almacenamiento de armas bacteriológicas (biológicas) y toxínicas y su destrucción (CAB), instrumento que contiene los pilares fundamentales para la regulación de este tipo de armamento (Pérez, 2004). A medida que la revolución biotecnológica siga avanzando con gran rapidez, los Estados continuarán respaldando este tipo de instrumentos para asegurarse de que sea regulada.

La biotecnología en el sector militar no solo se centra en la creación y el uso de armas químicas y tóxicas. Hoy busca la creación de herramientas tecnológicas por medio de organismos biológicos vivos y que generalmente han sido alterados para mejorar sus funciones (NTNU, s.f.). A continuación, se esbozan algunos proyectos de EE. UU. y China al respecto.

Tabla 2. Proyectos estadounidenses y chinos de biotecnología

Contribuyente	Avance biotecnológico
Estados Unidos	**Xenobots:** el mismo equipo que construyó los primeros robots vivos en 2020 descubrió que también son organismos con capacidad reproductiva. Estos pequeños robots pueden salir, encontrar células y construir copias de sí mismos. Michael Levin, PhD., profesor de biología y director del Allen Discovery Center en la Universidad de Tufts, mencionó que es una forma completamente nueva de reproducción biológica y diferente a la de cualquier animal o planta conocida (citado en Hunt, 29 de noviembre de 2021). Sus creadores han resaltado que tales máquinas pueden contribuir a combatir problemas como la polución, el cambio climático, las pandemias como el COVID-19 y enfermedades como el cáncer (Brown, 29 de noviembre de 2021).
China	**Quimeras:** un equipo de estadounidenses, chinos y españoles, liderado por Juan Carlos Izpisua, ha creado 132 embriones a partir de una mezcla de células de mono y humano que llegaron a crecer hasta 19 días fuera del útero. Su meta final es la creación de quimeras de cerdo y persona con la finalidad de generar órganos humanos en el ganado porcino para miles de pacientes que esperan un trasplante. Este trabajo tendría una variedad de aplicaciones en investigación y medicina regenerativa, según Izpisua (DW, 16 de abril de 2021).

Fuente: elaboración de los autores.

Tanto los xenobots como las quimeras tendrían una enorme contribución para la salud de los combatientes de guerra, pues se estima que en el futuro podrían ser usados para mejorar articulaciones, generar compuestos regenerativos como piel y órganos, detectar enfermedades, curar heridas e identificar y reemplazar células malignas. Aunque todavía no han tenido aplicaciones prácticas, la combinación de biología molecular e inteligencia artificial podría usarse potencialmente en el cuerpo y el medio ambiente, de acuerdo con las proyecciones científicas.

En relación a las cuatro estrategias de defensa, los desarrollos biotecnológicos ponen en evidencia lo siguiente. Las armas biológicas pueden llegar a tener un gran efecto disuasivo y psicológico en la guerra a pesar de las prohibiciones internacionales. El avance logrado por los EE. UU. en la década de 1960 y por la URSS en la década de 1980 sugiere que es muy probable que se haya desarrollado la capacidad de lanzar un ataque biológico con la equivalencia destructiva de un ataque nuclear. De hecho, en las próximas décadas, los ataques biológicos menos letales pueden volverse amenazas usuales (Buccina, George y Weber, 17 de septiembre de 2021). A medida que las potencias militares empiecen a prestar atención a la posibilidad de incurrir en armas biológicas más sutiles y precisas para evitar confrontaciones bélicas, otras naciones del mundo podrían seguir este juego, no solo por la amenaza que representan, sino por la transformación del orden mundial en la búsqueda de liderazgo biotecnológico.

Como estrategia de denegación estas armas no tienen mucho campo de acción. Su uso a lo largo del tiempo no ha tenido como propósito neutralizar o destruir las capacidades

militares del oponente, sino intimidar a los adversarios para conseguir objetivos específicos. La biotecnología configura la siguiente relación: cuando un país ve que su rival avanza en esta área, usa otros medios de disuasión para demostrar su capacidad de responder hasta lograr emular esta capacidad –o pretende hacerlo–, pero no puede frenar fácilmente la del otro y ello genera un contexto de competencia y de vulnerabilidad mutua o cooperación por la posibilidad de un escenario de conflicto. Mantener el secreto de fondo de estos desarrollos, filtrando solo una parte, y sumarse al esfuerzo público por prohibir los avances militares (del otro) usando el derecho internacional, es parte del juego.

En la estrategia de interferencia, la biotecnología encuentra un gran espacio. Los avances que se han dado, especialmente en biología sintética, proporcionan a los atacantes una variedad de armas que son cercanas a los mecanismos de guerra híbrida. Por ejemplo, el ántrax se ha visto como un arma biológica ideal, pues es una sustancia que cautelosamente libera esporas que causan una infección mortal una vez que se inhala. Si bien es un contexto imaginario, en caso de realizarse un ataque bioterrorista, el *Bacillus anthracis* (la bacteria que causa el ántrax) podría ser uno de los agentes biológicos que se utilizaría con más probabilidad (CDC, 2014). La biotecnología como estrategia de interferencia se entiende desde una perspectiva en la que participan actores no estatales e ilegales, así como *proxies*, buscando desestabilizar el orden doméstico de otro país.

Finalmente, estas armas se han usado, brutalmente, en la estrategia de castigo, en tanto que su empleo causa un daño insoportable o irreparable al enemigo. A pesar de que existen regímenes internacionales que pretenden frenar el uso de estas tecnologías con propósitos de castigo, el caso de la guerra civil en Siria demuestra el alcance de la biotecnología en este ámbito. Según el Departamento de Estado de EE. UU., en 2013 el régimen de Assad lanzó gas sarín sobre la sociedad civil en el distrito de Ghouta de Damasco, que mató a más de 1.400 sirios, muchos de ellos niños. Se estima que el régimen de Assad ha usado armas químicas contra el pueblo sirio al menos 50 veces desde que comenzó el conflicto (Price, 21 de agosto de 2021). El impacto de estas armas, a diferencia de las nucleares, es tardío e incluso puede extenderse por años, ya que su intención no es la aniquilación total ni alentar una confrontación militar.

Conclusiones y recomendaciones

La cuarta revolución industrial, con la integración de tecnologías mecanizadas, digitales y biológicas, en conjunción con sistemas avanzados de datos y de aprendizaje profundo e inteligencia artificial, están generando presiones de cambio inusitado en los asuntos militares. No solamente están cambiando los medios de la guerra al aumentar su velocidad, precisión y letalidad (en caso de las armas convencionales) y traer innovaciones en cuanto a armas no kinésicas, además de la posibilidad de su total automatización. Puede argumentarse que se

está produciendo una nueva revolución en asuntos militares (RMA), con patrones de transformación de doctrina, organización, tácticas, comando, control e inteligencia e, incluso, del perfil y las funciones del personal militar. Estos desarrollos están ampliando la brecha entre las potencias militares más avanzadas y el resto de los países. Empero, en un sistema internacional tendiente a la multipolarización, el mecanismo de emulación y la posibilidad de desarrollar y adquirir tecnologías de uso dual, hacen más factible su proliferación y así inducen una mayor inestabilidad.

Sin embargo, estos medios aún enfrentan dificultades en términos de eficiencia para cumplir los objetivos políticos, especialmente en el contexto de los conflictos asimétricos e híbridos, y no necesariamente resuelven las raíces o cuestiones de fondo que dan lugar a los enfrentamientos violentos internos e internacionales. En últimas, la planeación estratégica y la toma final de decisiones seguirán bajo el control de los seres humanos, aunque cuenten cada vez más con el insumo de las herramientas digitales, ya que las emociones y la intuición, así como la experiencia, siguen siendo factores estratégicos importantes, difícilmente replicables por las máquinas.

Se tiene un escenario internacional marcado por tres grandes potencias en materia de IA, pero con particularidades que permiten distinguir sus desempeños. En primer lugar, el perfil estadounidense, si bien parece ser el más claro de los tres analizados, aún tiene el reto de la financiación, así como también de la necesidad de arreglos institucionales que permitan realizar esfuerzos gubernamentales específicos en IA y brindar mejor acompañamiento, regulación y cooperación con el sector privado. China, por su parte, parece mostrar un rol más diplomático enfocado en la interacción de sus industrias con las de otros países, pero se ha comprobado que usa la IA como herramienta de desinformación y se beneficia del desvío de datos. Por último, se observa cómo Rusia ha mostrado vocación ofensiva y defensiva en sus desarrollos, al haber logrado modificaciones estatales para dar vía a sus proyectos en IA, sin embargo, se enfrenta a obstáculos en materia de financiación, más aún, con el desgaste del conflicto actual en Ucrania. De las estrategias de defensa, las de denegación e interferencia parecen ser a las que más puede recurrirse desde la IA.

La carrera espacial desde los tiempos de la Guerra Fría ha marcado un camino de avance constante y de fortalecimiento de capacidades por parte de los Estados. Teniendo en cuenta que han surgido otros actores importantes en el teatro de operaciones espaciales, y que las grandes potencias se han vuelto vulnerables por esto, el mundo de hoy se encuentra en una espiral de armamento espacial que ha sido denominada como un regreso a la Guerra Fría, pero multipolar. Tal escenario pone sobre la mesa la importancia de un régimen internacional que no solo se encargue de pautar los límites y/o fronteras ultraterrestres de los países, sino de seguir fortaleciendo las reglas de juego para garantizar la paz y la no soberanía en los cuerpos celestes. De las estrategias de defensa, la disuasión, la interferencia y la denegación parecen las más útiles en el desarrollo espacial militar.

Los misiles hipersónicos alteran los cálculos y sistemas tradicionales de defensa antibalística. Por la velocidad extrema que pueden alcanzar, su capacidad de volar a baja altitud y la posibilidad de ser maniobrados en el aire, resultan prácticamente imposibles de interceptar con la tecnología actual. En la competencia por su desarrollo, Rusia y China parecen llevar la ventaja sobre EE. UU., aunque no por mucho tiempo. El Congreso estadounidense ha aprobado varias partidas presupuestales para el logro de esta tecnología y también para desarrollar una constelación de pequeños satélites con cobertura planetaria y mayor capacidad de detectar esos lanzamientos desde su origen. Como en otras áreas, la clave para la superpotencia es la cooperación y coordinación con las empresas privadas de tecnologías de defensa, en lugar del monopolio de Estado. Sin embargo, en el actual contexto internacional, resulta más fácil el desvío y la captación de información reservada, incluso en materia de propiedad intelectual y avances tecnológicos, para provocar mayor posibilidad de copia y réplica.

La estrategia de disuasión nuclear, típica de la Guerra Fría, está siendo alterada por esa tecnología emergente. La posibilidad de un ataque nuclear inminente con poca capacidad de contramedidas es evidente. No obstante, este medio de guerra resulta vulnerable ante ataques cibernéticos y ante estrategias disruptivas como la de interferencia en los sistemas políticos de los países que lo tienen (o quieren). No resulta útil como medio de las estrategias de denegación ni de interferencia y tampoco de castigo, por sus efectos devastadores. Empero, en el contexto de la actual geopolítica inestable y disruptiva, es indispensable conocer a fondo la doctrina de defensa y nuclear de los países para poder hacer cálculos estratégicos acerca de su peligrosidad y posibilidad de uso. Asimismo, cabe la posibilidad de que actores no estatales (por ejemplo, terroristas) y *proxies* ataquen los sistemas de control y soporte digital de estos misiles, tanto con fines ideológicos como económicos, lo cual eleva los riesgos de posesión y transferencia de esta tecnología.

La biotecnología ha brindado herramientas al sector militar desde dos aristas importantes, pero aterradoras. Por un lado, el empleo de armamento químico ha transformado las reglas de la guerra convencional porque son armas económicas en comparación con otras armas de destrucción masiva y sus procesos de fabricación son relativamente sencillos. Por el otro, el resurgimiento de esta tecnología es capaz de mejorar los procesos e impactos de la guerra alrededor del mundo, tal y como ocurre con los xenobots y las quimeras. De las estrategias de defensa, la disuasión, la interferencia y el castigo parecen ser las que más se propician desde el desarrollo biotecnológico.

Finalmente, las implicaciones de las innovaciones mencionadas anteriormente para Colombia dependen de la posición geopolítica que tenga el Estado con los países desarrolladores. Tickner y Morales (2015) sugieren que Colombia y EE. UU. guardan una relación de cooperación dependiente, especialmente en torno a temas de seguridad. Surge como producto de la redistribución de funciones, originada en cambios en la política internacional de EE.UU. y

cuyo efecto principal es la transferencia de nuevos roles a países como Colombia, con cierto grado de experticia y afinidad. Allí hay una puerta para la transferencia de doctrina y tecnología, obviamente limitada a fenómenos y amenazas domésticos, regionales o transnacionales. Aún con la designación de Colombia como socio no miembro de OTAN y aliado estratégico de EE. UU. no miembro de OTAN, difícilmente el país suramericano, una potencia regional secundaria y apegada al derecho internacional, adquirirá o estará interesado en adquirir tecnologías emergentes en relación con estrategias de interferencia, denegación o castigo, siendo más racionales las disuasivas limitadas y preventivas.

Entretanto, las relaciones de Colombia con Rusia y China responden, principalmente, a vínculos económicos y comerciales, que pueden expandirse de forma limitada a aspectos puntuales –no estratégicos– de la industria de defensa en un mundo multipolar de oferentes y compradores. Lo anterior es consecuencia de un escenario económico globalizado. Sin embargo, la relación oscila entre la desarticulación y la discontinuidad, por cuenta de la relación estrecha que prefiere Colombia con EE. UU. (Rodríguez, 2019). Ello no debe implicar una actitud hostil o displicente de Colombia para con China o Rusia, sino más bien una constante postura al margen de conflictos militares entre grandes poderes. Como consecuencia, las implicaciones de las innovaciones tecnológicas de otros en seguridad y defensa para Colombia variarán dependiendo de quién las ostente, pero serán esencialmente indirectas hasta que tengan incidencia sobre sus hipótesis propias de conflicto, preocupando, por ejemplo, el efecto de los avances rusos y chinos sobre la capacidad militar de Venezuela. Allí se recomienda analizar de cerca, mediante herramientas de inteligencia avanzada, el progreso de las capacidades bélicas y de interferencia del régimen político dictatorial vecino, examinando si ha recurrido a instrumentos de las guerras híbrida y cognitiva para incidir en el sistema de decisiones y electoral de Colombia.

Tratándose de EE. UU., las implicaciones pueden reflejarse en una extensión de los conocimientos y avances para las FF. MM. colombianas en el desarrollo y mejoramiento de herramientas propias, con adaptaciones a necesidades particulares, como el combate al narcotráfico, la insurgencia, la minería ilegal y el contrabando, y la prevención y atención a desastres naturales y emergencias migratorias, como lo ofrecen las tecnologías espaciales y cibernéticas. El país tiene un campo enorme por desarrollar en estas dos áreas, con fines tanto civiles como militares, para tiempos de guerra y tiempos de paz, en aras del progreso económico y de la seguridad y defensa. En este sentido, los tomadores de decisión políticos y militares y los estrategas deben identificar las oportunidades más viables, menos onerosas, de las tecnologías duales emergentes que beneficiarán a Colombia según sus características como país en vías de desarrollo y consolidación interna, en un entorno mundial VICA (de volatilidad, incertidumbre, complejidad y ambigüedad). No obstante, para reducir la dependencia estratégica con la superpotencia, podría ser conveniente aprovechar o buscar complementos tecnológicos con países OTAN y con aliados estratégicos en la región, tales como Brasil

o México, con perspectiva de cooperación, transferencia e integración tecnológica regional de mutuo beneficio y en condiciones de equidad, sostenibilidad y transparencia.

El Estado colombiano debe seguir participando dinámicamente y del lado de las potencias democráticas en los escenarios multilaterales que discuten la prohibición, el uso y la regulación de armas autónomas y de destrucción masiva, además de propender por el uso pacífico y sin apropiación del espacio y los cuerpos celestes. El control humano de los sistemas de armas y de decisión debe persistir en todo momento por la amenaza en sí que representan los sistemas autónomos y no regulados (HRW, 2020). La diplomacia normativa y la diplomacia de la defensa con fines pacíficos, como la seguridad cooperativa, además de una mínima disuasión creíble y una inteligencia eficiente, son las mejores herramientas de estrategia para potencias secundarias e intermedias, que no tienen la capacidad de competir de frente con las principales potencias militares, y cuyo alineamiento geopolítico debe ser limitado en aras de su propia subsistencia e interés según la jerarquía que ocupan en el sistema.

Referencias

Alcocer, J. M. (2002). Biotecnología militar y antiterrorismo. *Ciencia UANL*, *V*(1), 85-90. Recuperado de: https://www.redalyc.org/pdf/402/40250114.pdf

Almeida, M. (2019). Robots, inteligencia artificial y realidad virtual: una aproximación en el sector del turismo. *Cuadernos de Turismo*, 44, 13-26.

Álvarez Montero, J. l. (2021). La nueva frontera del desarrollo espacial y los derechos humanos. *Revista de la Facultad de Derecho de la Universidad Veracruzana*, 4. Recuperado de: https://www.uv.mx/derecho/files/2019/04/Revista-de-la-Facultad-de-Derecho-No-4-La-nueva-frontera-del-desarrollo-espacial-y-los-derechos-humanos.pdf

Berrío, M. A. (2008). La seguridad espacial 50 años después del Sputnik. *Política Exterior*, *22*(123), 123-133. Recuperado de: https://www.jstor.org/stable/41806469

Bousquet, A. (2017). Revolution in Military Affairs? Changing Technologies and Changing Practices of Warfare. En D. R. McCarthy (Ed.), *Technology and World Politics: An Introduction* (pp. 1-21). Abingdon y Nueva York: Routledge. Recuperado de: https://core.ac.uk/download/pdf/199196752.pdf

Britannica. (s.f.a). *Denial military strategy*. Recuperado de: https://www.britannica.com/topic/denial-military-strategy

Britannica. (s.f.b). *Deterrence, political and military strategy*. Recuperado de: https://www.britannica.com/topic/deterrence-political-and-military-strategy

Brown, J. (29 de noviembre de 2021). Team builds the first living robots that can reproduce. *Wyss Institute*. Recuperado de: https://wyss.harvard.edu/news/team-builds-first-living-robots-that-can-reproduce/

Bryce, H. y Parakilas, J. (2018). Conclusions and Recommendations. En M. L. Cummings, H. M. Roff, K. Cukier, J. Parakilas y H. Bryce (Eds.), *Artificial Intelligence and International Affairs* (pp. 43-46). Londres: Chatham House, The Royal Institute of International Affairs.

Buccina, J.; George, D. y Weber, A. (17 de septiembre de 2021). Biological Deterrence for the Shadow War. *War on the Rocks*. Recuperado de: https://warontherocks.com/2021/09/biological-deterrence-for-the-shadow-war/

Cabrera-Ortiz, F. y Ospina-Gutiérrez L. M. (Eds.) (2021). *Estrategia de Seguridad Aérea y Espacial Nacional*. Bogotá: Escuela Superior de Guerra General Rafael Reyes

Prieto. Recuperado de: https://esdeguelibros.edu.co/index.php/editorial/catalog/view/101/123/1362

Capaccio, A. (12 de noviembre de 2021). Hypersonic Sticker Shock: U.S. Weapons May Run $106 Million Each. *Bloomberg*. Recuperado de: https://www.bloomberg.com/news/articles/2021-11-12/hypersonic-sticker-shock-u-s-weapons-may-run-106-million-each

Castro, J. (20 de abril de 2022). Un nuevo paso hacia una pesadilla nuclear en Europa. *Documento Análisis Instituto Español de Estudios Estratégicos*, 27/2022. Recuperado de: https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA27_2022_JOSCAS_Nuclear.pdf

Catrinel, A. I. (2022). The Security Impact of the Militarization of Outer Space. *Bulletin of Carol I National Defence University*, 16-31. Recuperado de: https://revista.unap.ro/index.php/bulletin/article/view/1417/1365

CDC [Centers for Disease Control and Prevention]. (2014). *El ántrax. Bioterrorismo*. Recuperado de: https://www.cdc.gov/anthrax/es/bioterrorismo/bioterrorismo.html

Chandra, B. (15 de febrero de 2021). Collaboration or Chaos: Two Futures for Artificial Intelligence and US National Security. *Modern War Institute*. Recuperado de: https://mwi.usma.edu/collaboration-or-chaos-two-futures-for-artificial-intelligence-and-us-national-security/

Cukier, K. (2018). The Economic Implications of Artificial Intelligence. En M. L. Cummings, H. M. Roff, K. Cukier, J. Parakilas y H. Bryce (Eds.), *Artificial Intelligence and International Affairs* (pp. 29-42). Londres: Chatham House, The Royal Institute of International Affairs.

Cummings, M. (2018). Artificial Intelligence and the Future of Warfare. En M. L. Cummings, H. M. Roff, K. Cukier, J. Parakilas y H. Bryce (Eds.), *Artificial Intelligence and International Affairs* (pp. 7-18). Londres: Chatham House, The Royal Institute of International Affairs.

Dash, D. (2018). *Autonomy and Artificial Intelligence: The Future Ingredient of Area Denial*. Recuperado de: https://www.semanticscholar.org/paper/Autonomy-and-Artificial-Intelligence-%3A-The-Future-Dash/f6adf6e580ada281b5f1a68992fb51d92e5fd135

DARPA [Defense Advanced Research Projects Agency]. (s.f.). *Innovation in Biotechnology*. Recuperado de: https://www.darpa.mil/about-us/innovation-in-biotechnology

Díaz, J. (13 de julio de 2021). China desarrolla una nueva arma espacial contra la que EEUU no tiene defensa. *El Confidencial*. Recuperado de: https://www.elconfidencial.com/tecnologia/novaceno/2021-07-13/china-guerra-espacial-estados-unidos-pentagono_3181083/

DW [Deutsche Welle]. (16 de abril de 2021). *Científicos crean en China "embriones quimera" con mezcla de mono y humano*. Recuperado de: https://www.dw.com/es/cient%C3%ADficos-crean-en-china-embriones-quimera-con-mezcla-de-mono-y-humano/a-57228801

DW [Deutsche Welle]. (2 de marzo de 2022). *"Casus belli": jefe de la agencia espacial rusa dice que el hackeo de sus satélites justificaría la guerra*. Recuperado de: https://www.dw.com/es/el-jefe-de-la-agencia-espacial-rusa-dice-que-el-hackeo-de-sus-sat%C3%A9lites-justificar%C3%ADa-la-guerra/a-60989389

Elliott, V. (14 de marzo de 2022). In Ukraine's cyber-war with Russia, who is a civilian and what is a war crime? *Rest of World*. Recuperado de: https://restofworld.org/2022/in-ukraines-cyber-war-with-russia-who-is-a-civilian-and-what-is-a-war-crime/

Erwin, S. (15 de marzo de 2022). DoD estimates $2.5 billion price tag for global constellation to track hypersonic missiles. *Space News*. Recuperado de: https://spacenews.com/dod-estimates-2-5-billion-price-tag-for-global-constellation-to-track-hypersonic-missiles/

Freund, A. (10 de mayo de 2021). Agente naranja: la larga sombra de la guerra de Vietnam. *DW*. Recuperado de: https://www.dw.com/es/agente-naranja-la-larga-sombra-de-la-guerra-de-vietnam/a-57486571

Futter, A. (2020). The Risks Posed by Emerging Technologies to Nuclear Deterrence. Perspectives on Nuclear Deterrence in the 21st Century. *Chatam House Research Paper*. Recuperado de: https://www.chathamhouse.org/2020/04/perspectives-nuclear-deterrence-21st-century-0/risks-posed-emerging-technologies-nuclear

Goldberg, J. (10 de enero de 2020). Watch Russia, China, United States race to deploy 'blazingly fast' hypersonic weapons. *Science*. Recuperado de: https://www.science.org/content/article/watch-russia-china-united-states-race-deploy-blazingly-fast-hypersonic-weapons

Hammes, T. (24 de agosto de 2018). *4IR Changes the Character of War*. Institute for National Strategic Studies and National Defense University, United States. Recuperado de: https://researchcentre.army.gov.au/sites/default/files/tx_hammes_-_4ir_changes_the_character_of_war.pdf

Haney, B. S. (2020). Applied Artificial Intelligence in Modern Warfare and National Security Policy. *Hastings Science and Technology Law Journal*, *11*(1), 61-100.

HRW [Human Rights Watch]. (2020). *Stopping Killer Robots, Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control*. Recuperado de: https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and#_ftn69

Hunt, K. (29 de noviembre de 2021). World's first living robots can now reproduce, scientists say. *CNN*. Recuperado de: https://www.cnn.com/2021/11/29/americas/xenobots-self-replicating-robots-scn/index.html

Infobae. (29 de diciembre de 2018). *Qué son y cómo funcionan los misiles hipersónicos y por qué Estados Unidos, Rusia y China compiten por ellos*. Recuperado de: https://www.infobae.com/america/mundo/2018/12/29/que-son-y-como-funcionan-los-misiles-hipersonicos-y-por-que-estados-unidos-rusia-y-china-compiten-por-ellos/

Jing, Y. (28 de diciembre de 2021). How Does China Aim to Use AI in Warfare? *The Diplomat*. Recuperado de: https://thediplomat.com/2021/12/how-does-china-aim-to-use-ai-in-warfare/

Kainikara, S. (2013). Air Power and the Strategy of Punishment. *Royal Australian Air Force, Air Power Development Centre Working Paper*, 36. Recuperado de: https://airpower.airforce.gov.au/sites/default/files/2021-03/WP36-Air-Power-and-the-Strategy-of-Punishment.pdf

Kamarck, E. (29 de noviembre de 2018). Malevolent soft power, AI, and the threat to democracy. *Brookings*. Recuperado de: https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy/

López, L. I. (2010). La seguridad aeroespacial en América del Norte. *Norteamérica*, *5*(1), 173-219. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35502010000100007&lng=es&tlng=es

Mallick, Pk. (2020). *Revolutions in Military Affairs (RMA) an Apprisal*. Recuperado de: https://www.researchgate.net/publication/344737633_REVOLUTIONS_IN_MILITARY_AFFAIRS_RMA_AN_APPRISAL

Min, X.; David, J. y Suk, K. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research*, *9*(2), 90-95. Recuperado de: https://www.researchgate.net/publication/323638914_The_Fourth_Industrial_Revolution_Opportunities_and_Challenges

Nelson, N.; Speranza, L.; Deni, J. R.; Alden, C.; Brattberg, E.; Cliff, R.; Duckenfield, M. y Ellis, R. E. (2022). Security Risks: Dual-Use Technology in Europe. En *China, Europe, and the Pandemic Recession: Beijing's Investments and Transatlantic Security* (pp. 151-198). Carlisle, Pensilvania: Strategic Studies Institute, US Army War College. Recuperado de: https://www.jstor.org/stable/resrep40643.11

NTNU [Norwegian University of Science and Technology]. (s.f). *What is Biotechnology?* Recuperado de: https://www.ntnu.edu/ibt/about-us/what-is-biotechnology

Perasso, V. (12 de octubre de 2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). *BBC*. Recuperado de: https://www.bbc.com/mundo/noticias-37631834

Pérez, J. R. (2004). El Derecho Internacional ante las nuevas armas biológicas. *Revista Española de Derecho Militar*, 84, 61-90. Recuperado de: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/redm_084.pdf#page=61

Price, N. (21 de agosto de 2021). Syria: Eighth Anniversary of the Ghouta Chemical Weapons Attack. *U.S. Department of State*. Recuperado de: https://www.state.gov/syria-eighth-anniversary-of-the-ghouta-chemical-weapons-attack/

Rodríguez Robayo, S. (2019). *Relaciones bilaterales entre Colombia y la República Popular China: aspectos estratégicos durante la última década (2008-2018)* (trabajo de investigación, departamento de Ciencia Política y Relaciones Internacionales). Universidad de Bogotá Jorge Tadeo Lozano, Bogotá. Recuperado de: https://expeditiorepositorio.utadeo.edu.co/handle/20.500.12010/7857

Romero M. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval*, *16*(1), 51-70.

Ryan, M. (31 de octubre de 2018). *War and the 4th Industrial Revolution: Developing the Future Intellectual Edge*. Presentación ante The Military Education Coordination Council. Recuperado de: https://www.jcs.mil/Portals/36/Documents/Doctrine/MECC2018/australian_defence_college_briefing.pdf?ver=2018-10-22-095806-923

Sayler, K. (20 de julio de 2022). Hypersonic Weapons: Background and Issues for Congress. *Congressional Research Service*. Recuperado de: https://sgp.fas.org/crs/weapons/R45811.pdf

Shea, J. (20 de abril de 2020). Perspectives on Nuclear Deterrence in the 21st Century. *Chatam House Research Paper*. Recuperado de: https://www.chathamhouse.

org/2020/04/perspectives-nuclear-deterrence-21st-century-0/risks-posed-emerging-technologies-nuclear

Steer, C. (2017). Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space. *Georgetown Journal of International Affairs*, *18*(1), 9-16. doi:10.1353/gia.2017.0003

Steer, C. (8 de enero de 2020). Why Outer Space Matters for National and International Security. *ANU College of Law Research Paper*, 20.25. Recuperado de: https://ssrn.com/abstract=3604805

Stone, R. (8 de enero de 2020). 'National pride is at stake'. Russia, China, United States race to build hypersonic weapons. *Science*. Recuperado de: https://www.science.org/content/article/national-pride-stake-russia-china-united-states-race-build-hypersonic-weapons

Thomas, Z. (23 de marzo de 2022). Banks' Use of A.I. Raises Risk of Cyberattacks by Russia, Experts Say. *The Wall Street Journal Podcasts*. Recuperado de: https://www.wsj.com/podcasts/tech-news-briefing/banks-use-of-ai-raises-risk-of-cyberattacks-by-russia-experts-say/7732e044-cb65-496d-bc25-fee48bdc7d01

Tickner, A. y Morales, M. (2015). Cooperación dependiente asociada. Relaciones estratégicas asimétricas entre Colombia y Estados Unidos. *Colombia Internacional*, 85, 171-205.

Wigell, M.; Mikkola, H. y Juntunen, T. (2021). *Best practices in the whole-of-society approach in countering hybrid threats*. Bruselas: Directorate General for External Policies of the European Parliament. Recuperado de: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf

Wong, Y. H.; Yurchak, J.; Button, R. W.; Frank, A. B; Laird, B.; Osoba, O. A.; Steeb, R.; Harris, B. N. y Joon Bae, S. (2020). *Deterrence in the Age of Thinking Machines*. Santa Mónica, CA: RAND Corporation. Recuperado de: https://www.rand.org/pubs/research_reports/RR2797.html