OASIS
OBSERVATORIO DE ANÁLISIS DE LOS SISTEMAS INTERNACIONALES

Oasis
ISSN: 1657-7558
ISSN: 2346-2132
Universidad Externado de Colombia

Peña, Nicolás De la; Granados, Oscar
Cuarta revolución industrial: implicaciones en la seguridad internacional1
Oasis, núm. 33, 2021, Enero-Junio, pp. 29-48
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/16577558.n33.05

Disponible en: https://www.redalyc.org/articulo.oa?id=53169984004

Cuarta revolución industrial: implicaciones en la seguridad internacional[1]

Nicolás De la Peña*
Oscar Granados**

RESUMEN

Esta investigación analiza las implicaciones de la cuarta revolución industrial en la seguridad internacional. Considera los impactos en conjunto de las tecnologías como una perspectiva multidimensional de la seguridad, la perspectiva expansiva de la seguridad y la innovación disruptiva. Se encuentra que las tecnologías amplían las capacidades actuales y crean otras nuevas para los actores tradicionales y no tradicionales. Así, la seguridad internacional se expande horizontalmente dado el surgimiento de amenazas que supone el ámbito digital en las dimensiones de la seguridad, y verticalmente al transformar las capacidades de los actores del sistema internacional.

Palabras clave: seguridad internacional, tecnologías, cuarta revolución industrial, inteligencia artificial, relaciones internacionales.

---

[1] Este artículo surge de la tesis de maestría presentada para optar al título de Magíster en Asuntos Internacionales por la Universidad Externado de Colombia. La disertación obtuvo distinción meritoria y fue dirigida por el profesor Oscar Granados.

* Magíster en asuntos internacionales, profesional en comercio internacional. Profesor de tiempo completo, Universidad de La Salle, Facultad de Ciencias Económicas y Sociales. (Colombia). [ndelapena@unisalle.edu.co]; [ORCID: 0000-0001-7223-9502].

** Candidato a doctor en ciencias sociales, magíster en relaciones internacionales, magíster en asuntos internacionales, especialista en negocios internacionales, economista. Profesor de tiempo completo, Universidad Jorge Tadeo Lozano, Departamento de Economía y Comercio Internacional. (Colombia). [oscarm.granadose@utadeo.edu.co]; [ORCID: 0000-0002-4992-8972].

Recibido: 1 de marzo de 2020 / Modificado: 18 de mayo de 2020 / Aceptado: 3 de junio de 2020

Para citar este artículo:

De la Peña, N. y Granados, O. (2021). Cuarta revolución industrial: implicaciones en la seguridad internacional. *OASIS*, 33, pp. 49-73.

DOI: https://doi.org/10.18601/16577558.n33.05

Fourth industrial revolution: implications for international security

ABSTRACT

This research analyzes the implications of the fourth industrial revolution on international security. It considers the impacts of the technologies as a whole drawing on the multidimensional perspective of security, the expansive perspective of security and the disruptive innovation framework. We found that new technologies increase current capabilities and create new ones for traditional and non-traditional actors. Therefore, international security expands horizontally by deepening the threat of the digital sphere in the security dimensions, and vertically by transforming the capabilities of international system actors.

Keywords: International security, technology, fourth industrial revolution, artificial intelligence, international relations.

1. INTRODUCCIÓN

La revolución tecnológica está transformando el mundo, integrando diversas disciplinas y conocimientos que, hasta hace algunos años, era impensable conectarlos de alguna forma. La inteligencia artificial (AI), la robótica, la impresión 3D, el internet de las cosas (IoT) y la biología sintética –por mencionar algunos– permiten una interacción entre los ámbitos físico, computacional, digital y biológico (Schwab, 2016). Pero ¿qué implicaciones presentan las nuevas tecnologías en la seguridad internacional? Los cambios que están surgiendo dan lugar al empoderamiento de nuevos actores, al aumento de sus capacidades y la aparición de nuevos escenarios. Estudios anteriores sobre la cuarta revolución industrial se han enfocado principalmente en las consecuencias económicas (Brynjolfsson & McAfee, 2014; Frey, 2019), empresariales (Agrawal, Gans & Goldfarb, 2019), éticas (Hooker & Kim, 2019), diplomáticas (Bjola & Holmes, 2015) y sociales (Makridakis, 2017), pero el tema no se ha abordado a profundidad desde las relaciones internacionales y, cuando se ha hecho, únicamente se toma como referente una tecnología de manera aislada (Cummings *et al*., 2018; Greg & Chan, 2017; Johnson, 2019; Scharre, 2018), enfatizando en actores específicos (Cronin, 2020) u observando los efectos en la guerra y el ámbito militar (Kosal, 2020; Tinnirello, 2018). No obstante, la verdadera transformación ocurre al entender las tecnologías como un sistema adaptativo complejo, cuyas propiedades emergentes superan la suma de sus partes.

Históricamente, el desarrollo tecnológico ha tenido implicaciones en la seguridad internacional. Estos desarrollos han otorgado ventajas a aquellos que han implementado y adoptado los nuevos inventos. La primera revolución industrial generó un crecimiento económico y un poderío militar que constituyó la consolidación del imperio británico. La segunda revolución industrial empoderó a varios Estados europeos, en especial al imperio alemán de Guillermo II. La tercera revolución industrial dio lugar a la consolidación de la hegemonía tecnológica y militar de Estados Unidos. Ahora, ¿cuáles son las implicaciones

de la cuarta revolución industrial en la seguridad internacional? Para ello, se realiza un análisis desde la perspectiva de la seguridad multidimensional, entendiendo dónde ocurre la transformación (dimensiones de seguridad), quién se transforma (objetos de referencia), qué ocurre (expansión horizontal y vertical) y cómo ocurre (redistribución de poder a partir de la innovación disruptiva).

Este documento está estructurado de la siguiente manera. Después de la presente introducción, se presenta un marco conceptual y metodológico que permite comprender las implicaciones del cambio tecnológico en la seguridad internacional y su aplicación en la investigación. A continuación, se discuten los resultados de la interacción de las tecnologías en las dimensiones de la seguridad internacional y, finalmente, se concluye.

2. MARCO CONCEPTUAL Y METODOLÓGICO

Para lograr el objetivo general de la investigación, se presenta una metodología que permite comprender qué cambio ocurre (expansión de la seguridad) dónde ocurre (dimensiones de seguridad) a quién le ocurre (objetos de referencia / actores) y por qué ocurre (innovación disruptiva). Por lo tanto, se presenta primero el marco conceptual que permite comprender la transformación de las tecnologías en la seguridad internacional, y basado en ello, se presenta la metodología.

Las transformaciones históricas de la seguridad internacional pueden comprenderse mediante la seguridad extendida propuesta por Rothschild (1995). La expansión vertical abarca la ampliación de los referentes de seguridad, que han pasado de estar centrados exclusivamente en el Estado –o las entidades políticas– a incluir otros actores del sistema internacional y los individuos. La expansión horizontal aborda las dimensiones de seguridad involucradas: desde lo militar hasta lo económico y lo social. Por lo tanto, se evidencia que históricamente, la seguridad se ha expandido al incorporar un mayor número de actores y asuntos que interactúan en la seguridad internacional, confirmando que esta es un sistema complejo. No obstante, se requiere una aproximación teórica que elabore con precisión dónde ocurren los cambios (asuntos) y a quién le ocurren (actores). A continuación, se presentan las principales teorías de los estudios de seguridad en relaciones internacionales.

El objetivo de los estudios de seguridad es analizar cómo son amenazados y cómo se protegen los objetos de referencia[2]. Desde el surgimiento de los estudios de seguridad y, en particular, durante la guerra fría, el objeto de referencia ha sido el Estado, que se asegura mediante la fuerza militar. Sin embargo, la seguridad internacional es un concepto contestado en relaciones internacionales (Baldwin, 1997) de modo que existen múltiples teorías que varían en función de los objetos de refe-

[2] En el contexto de la seguridad internacional, el objeto de referencia es entendido como "la protección de algo, frente a una amenaza de algún tipo" (Collins, 2007, p. 426).

rencia, considerando como variables los actores (quién realiza la acción y quién se defiende) y las amenazas (cómo realiza la acción y de qué se defiende). Los referentes de seguridad propuestos por el positivismo –realismo y liberalismo– consideran al Estado como el único referente de seguridad o, al menos, como el más relevante, aunque este último le otorga un carácter interdependiente en relación con elementos como el comercio y las finanzas. El origen de las amenazas se limita a la acción por parte de otros Estados, aunque el liberalismo considera que pueden limitarse mediante la cooperación y las instituciones (Frasson-Quenoz, 2014). Estas aproximaciones tradicionales no permiten considerar actores diferentes al Estado en los procesos de transición del poder, de modo que resultan inadecuados para la propuesta de este documento. Por otro lado, las aproximaciones no tradicionales, pese a que no poseen un cuerpo homogéneo de teorías, comparten como un *ethos* común la crítica a las aproximaciones tradicionales. Por ejemplo, consideran cómo se forma una amenaza, qué relación existe con ámbitos no militares o cómo influyen los actores no estatales (Mutimer, 2007). Teorías tales como los estudios de paz, estudios de género y la seguridad humana, tienen como referente de seguridad otros elementos como la población, el individuo y el medioambiente, buscando identificar causas estructurales de violencia y considerando que el Estado no es el referente central de la seguridad. Pero estas aproximaciones resultan difusas en su aplicación y están más enfocadas en explicar cómo se constituyen los asuntos de seguridad que en proveer herramientas para explicar las transformaciones (Browning, 2011).

En consecuencia, la Escuela de Copenhague (Buzan, Weaver & de Wilde, 1998) resulta pertinente porque es más concreta y menos heterogénea que otras aproximaciones críticas, y considera diversos actores (sistema internacional, Estado e individuos), a diferencia de las aproximaciones tradicionales. Esta teoría combina, por un lado, el concepto de dimensiones de seguridad: militar, económica, política, societal y ambiental[3] (Buzan, 1983), lo que permite comprender los objetos de referencia y las fuentes de las amenazas y, por otro lado, el concepto de securitización (Weaver, 1995), que sostiene que la definición de un asunto de seguridad es un acto discursivo. Dado el carácter exploratorio de este documento, se enfoca en las dimensiones de la seguridad internacional y sus condiciones materiales (Buzan, 1983), más no en las prácticas discursivas (Weaver, 1995), misma razón por la cual enfoques sociohistóricos (por ejemplo: Buzan, 2015) no pueden ser aplicados en este trabajo. La Escuela de Copenhague permite incorporar los cambios que ocurren en términos de actores y dimensiones de la seguridad internacional.

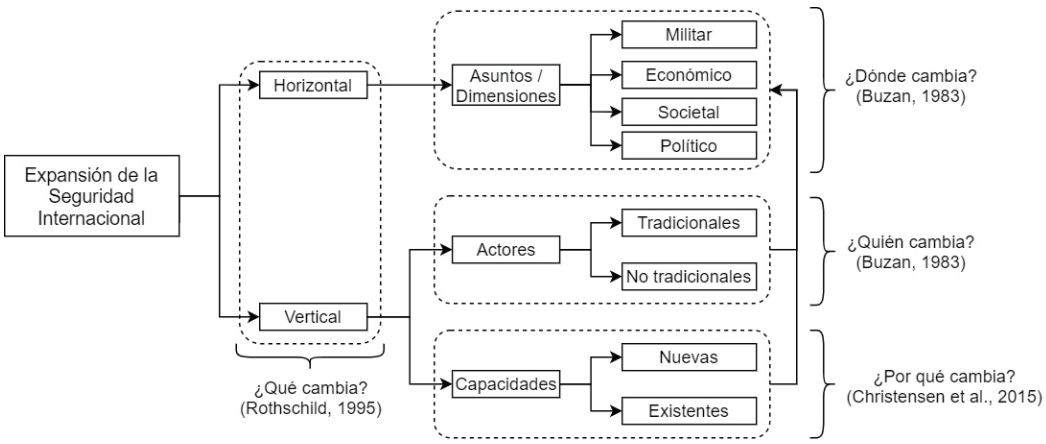
Ahora bien, la interacción entre los actores del sistema internacional es dinámica y la tecnología es un factor que propicia el cambio

[3] En la presente investigación, los sectores de la seguridad definidos por Buzan son considerados como *dimensiones* de seguridad.

y la redistribución del poder, afectando así las dimensiones y expandiendo la seguridad internacional. Para estudiar este fenómeno, se aplica el marco analítico de la innovación disruptiva de (Christensen, Raynor & McDonald, 2015) que, aunque inicialmente fue creado para comprender los cambios en la participación empresarial en el mercado, es posible su aplicación para el estudio de los cambios en la participación de actores internacionales en el sistema internacional (Cronin, 2020). Sostiene que la transformación de un producto caro y exclusivo en otro asequible y masivo –usualmente como consecuencia de nuevas tecnologías– genera redistribuciones en la participación. En el sistema internacional esto supone que tecnologías y capacidades que antes eran exclusivas de ciertos actores ahora están distribuidas como consecuencia de la innovación. Esta se puede categorizar en sostenida y disruptiva, en la que la primera amplía las capacidades existentes de los actores y la segunda genera capacidades nuevas[4]. En términos generales, la disrupción provocada por las tecnologías genera una redistribución del poder entre diferentes actores y dimensiones de la seguridad internacional.

El marco conceptual permite comprender la expansión de la seguridad internacional (ver figura 1) con lo cual resulta posible establecer la metodología de trabajo: se examinan las transformaciones que ocurren en las cuatro

Figura 1
Marco conceptual



Fuente: Elaboración propia.

[4] En el resto del documento, se entenderá por aumento de capacidades la innovación sostenida, y por creación de capacidades nuevas la innovación disruptiva.

dimensiones de la seguridad internacional, analizando en cada una los cambios en los actores como consecuencia de la variación en sus capacidades.

3. RESULTADOS: IMPLICACIONES DE LAS NUEVAS TECNOLOGÍAS EN LA SEGURIDAD INTERNACIONAL

La seguridad internacional se estudia desde cuatro dimensiones con la finalidad de establecer las transformaciones que allí surgen como consecuencia de la transición del poder entre diversos actores que modifican sus capacidades. A continuación, se presentan las cuestiones más relevantes que transforman las capacidades de los actores en cada una de las dimensiones.

3.1. Seguridad militar

En esta sección se presentan los impactos que tienen las tecnologías de la cuarta revolución industrial en la seguridad militar. Inicialmente, se analizan los sistemas autónomos, los cuales reducen los costos para realizar un ataque e incrementan las capacidades de este. Posteriormente, se analiza el tema de la vigilancia y seguimiento, que se hace posible gracias al ecosistema digital que provee el IoT, así como la proliferación de armas de fuego, la cual se puede incrementar por tecnologías como la impresión 3D. Finalmente, en lo que respecta a las armas de destrucción masiva, tanto las impresoras 3D como la biología sintética plantean amenazas al crear capacidades nuevas o al incrementar el riesgo ya existente.

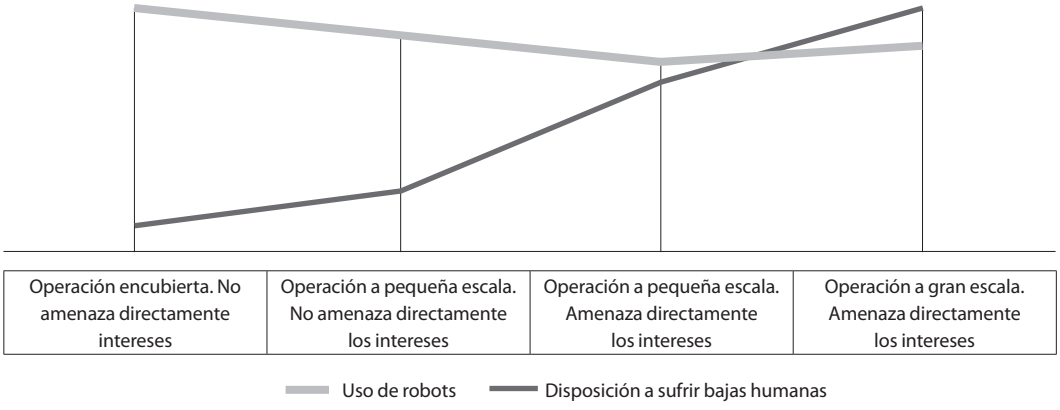
– Sistemas autónomos

La capacidad de hacer daño a distancia sin involucrar personal en las operaciones ha estado presente en los actores estatales y no estatales. No obstante, los sistemas autónomos amplían las capacidades actuales al no requerir la presencia física del operador dentro del aparato, reduciendo los riesgos humanos e incrementando la precisión en los procedimientos. El caso de los vehículos aéreos no tripulados (VANT) –popularmente llamados drones–, resulta ilustrativo. Estos han sido utilizados desde 1990 por parte de los Estados. Su proliferación entre actores estatales y no estatales es evidente, pues en el 2000 eran utilizados por 17 países mientras que la cifra ascendió a 75 en 2015 (Kreps, 2016). Esto se explica por el avance de los sensores que recopilan datos, los sistemas de procesamiento de información y los desarrollos en robótica, lo que les permite realizar ataques, hacer reconocimiento del terreno e incluso identificar patrones de comportamiento durante los sobrevuelos realizados (Oh *et al.*, 2014). Estas características, sumadas a la reducción de precios (PwC, 2018), han generado incentivos para que los actores no estatales utilicen VANT en sus operaciones como los casos de rebeldes libios y sirios, peshmergas kurdos, Hamas, Isis y los carteles de droga en Colombia y México (New America Foundation, 2017). Por ejemplo, Hezbollah en El Líbano y Siria (Franke, 2016) e Isis en Irak adaptaron drones de uso comercial para lanzar morteros y ejercer vigilancia, lo que les ha permitido obtener información que previamente era difícil de conseguir (Ward, 2017).

En consecuencia, "la ventaja tecnológica en los sistemas no tripulados, que una vez tuvo una élite reducida, está desapareciendo rápidamente" (Patterson, 2017, p. 24). Al tener una mejor capacidad de acción y estar expandida entre los actores no estatales, los ataques pueden volverse más factibles (Singer, 2009; Scharre 2018), aunque permiten mejorar la proporcionalidad (ataque limitado a cumplir el objetivo evitando el daño innecesario), y la discriminación, que busca reducir el daño colateral (Kreps, 2016). En ese sentido, el auge de los robots en el ámbito militar continuará, dado que la disposición a la pérdida en el caso de robots es muy inferior frente a las pérdidas humanas, además del costo comparativamente bajo que tienen estos frente a las tropas (McCafferty, 2016). Sin embargo, cuando hay amenazas significativas hacia un Estado, la sociedad está dispuesta a sacrificar vidas. La gráfica 1 pone de manifiesto esta relación y además permite observar cuándo serían útiles los robots militares.

El uso de sistemas autónomos y semiautónomos en el ámbito militar plantea, entonces, tres aspectos. En primer lugar, el hecho de que las operaciones sean realizadas por máquinas, mientras que los humanos las controlan en lugares remotos y seguros, permite realizar ataques y recolectar información sin poner en riesgo la integridad física de los atacantes, incrementa las capacidades actuales para los actores tradicionales y no tradicionales. En segundo lugar, el uso masivo de datos y sistemas de IA hacen que la precisión se incremente, ampliando así capacidades ya existentes. Finalmente, las dos características anteriores hacen que se reduzcan los costos económicos y en vidas de los ataques, incrementando la facilidad de que actores tradicionales y no tradicionales los realicen.

Gráfica 1
Situaciones de seguridad en las cuales es aceptado el uso de robots



Fuente: Adaptación propia con base en McCafferty (2016).

– Vigilancia y seguimiento

De otro lado, las capacidades de vigilancia y seguimiento se incrementan por la conectividad y el internet ubicuo que permite el IoT. Los sensores de detección han ganado precisión y facilidad de comunicación, pudiendo ser instalados en lugares remotos. El uso más destacado ha sido el monitoreo de fronteras, pues son capaces de detectar personas mediante sistemas de detección visual y auditivos. La disponibilidad continua de datos permite tomar decisiones basadas en análisis en tiempo real. No obstante, el hecho de que los objetos militares se encuentren en línea genera también riesgos, a saber: control remoto ilegal, robo de información, colocación de información falsa y perturbación del flujo de datos (Fraga-Lamas *et al.*, 2016), lo que puede ser ocasionado por actores no estatales (Cronin, 2020).

Por otra parte, la IA está cambiando los servicios de inteligencia, pues tiene la capacidad de detectar con mayor precisión "el movimiento potencialmente hostil de tropas cerca de una frontera nacional" (Kaplan, 2016, p. 117). ¿Qué explica este fenómeno? Primordialmente, que la información que se requiere para tomar decisiones surge de la recolección de datos. Pero el volumen es tal, que para obtener información son necesarios sistemas de IA y estructuras algorítmicas. Aun así, dado el nivel actual del *Big Data* (que no contempla todos los datos posibles), los analistas humanos seguirán siendo necesarios, pues son los únicos que pueden interpretar aquello que no está en los datos y ponerlo en contexto. Por lo tanto, la colaboración entre algoritmos y humanos es fundamental en este ámbito (Puyvelde, Coulthart & Hossain, 2017).

La vigilancia y el control ejercidos mediante tecnologías amplían las capacidades actuales, en especial, para los actores tradicionales y les permite a los actores no tradicionales utilizar las vulnerabilidades en los sistemas para realizar ataques.

– Proliferación de elementos bélicos

La impresión 3D amplía capacidades existentes y crea capacidades nuevas, pues permite obtener materiales en menos tiempo y con menos conocimiento previo, puesto que ya no se requiere el diseño y la preparación del proceso productivo, sino que basta con obtener los insumos y el archivo digital (Walther, 2015). Además, permiten, primero, copiar los diseños de las armas más avanzadas, reduciendo la ventaja que otorgaba el desarrollo y la posesión exclusiva de armamento avanzado, y segundo, la proliferación de estos hacia otros actores. Esto se conoce como proliferación horizontal, mientras la vertical se relaciona con la obtención de más elementos que ya se poseían previamente (Lodgaard, 1991).

La impresión 3D es un riesgo potencial para los Estados puesto que es una tecnología de doble uso (DoD, 2016). Por un lado, facilita la producción de componentes que le pueden ser útiles a las fuerzas armadas que, por ejemplo, han utilizado esta tecnología para producir piezas de repuesto en lugares de difícil acceso o con una cadena logística demorada como Afganistán (Gershenfeld, 2013). Pero, por otro lado, reduce la ventaja

tecnológica de sus fuerzas al facilitar la copia de algunos avances a otros actores estatales y no estatales.

La facilidad que da la impresión 3D para elaborar armas de forma rápida y a bajo costo, se hace evidente en la fabricación de pistolas y fusiles de asalto. En Estados Unidos para el 2013, se realizó una prueba de una pistola 9 milímetros fabricada totalmente –salvo el gatillo– en plástico utilizando una impresora 3D. El archivo digital con el cual se elaboró el arma ha sido descargado más de 100.000 veces y es posible encontrarlo en diferentes sitios web. También es posible encontrar el archivo con la información para la fabricación de una AK-47 (Robertson, 2013). De igual modo, un revólver de plástico se puede fabricar utilizando una impresora 3D de bajo costo –unos USD 500–. La munición se encuentra también entre los elementos bélicos que es posible imprimir (Kleinman, 2013)[5].

Así las cosas, la impresión 3D amplía las capacidades existentes –pues actores tradicionales y no tradicionales han tenido acceso a las armas desde tiempo atrás– al reducir tiempo y costos de procesos de fabricación. De igual modo, la reducción del conocimiento necesario para desarrollar nuevos objetos, crear nuevas capacidades y difundirlo hacia otros actores, incluidos los no estatales.

– Armas de destrucción masiva

Otra amenaza que surge de la impresión 3D es la disminución de la dificultad para la creación de componentes para armas de gran escala como motores de reacción y componentes de misiles, además de permitir la elaboración de componentes para la fabricación de armas de destrucción masiva, bien sea nucleares, químicas o biológicas, con el agravante de mantener dichas operaciones con un nivel de privacidad elevado (Kroenig & Volpe, 2015). Aunque actualmente es técnicamente imposible utilizar la manufactura aditiva para crear totalmente armas de destrucción masiva, Fey (2017) presenta cuatro maneras en los que esta tecnología puede contribuir al desarrollo de este tipo de armas, como se presenta en la Tabla 1.

De esta forma, la impresión 3D crea una nueva capacidad por la facilidad para la producción de componentes de las armas de destrucción masiva, junto con la privacidad que permite la fabricación personalizada, pues no son necesarias grandes fábricas, lo que reduce el desplazamiento originado por el comercio de estas piezas entre países, lo cual es uno de los principales factores para que los Estados monitoreen e identifiquen estas actividades.

Otras amenazas a la seguridad militar son causadas por la biología sintética porque "incrementa el riesgo de la creación de agentes

[5] Armas más sofisticadas, como los misiles, ya están en vía de ser logrados totalmente a través de impresoras 3D; Raytheon el fabricante estadounidense de armas informó que había producido el 80 por ciento de las partes de un misil utilizando manufactura aditiva (Raytheon, 2015). Por otro lado, la fabricación de drones en 3D también ha resultado exitosa, pues algunos investigadores lograron imprimir un dron en menos de un día a un costo aproximado de USD 2.500 (Fey, 2017).

Tabla 1
La impresión 3D facilita el desarrollo de armas de destrucción masiva

Fácil obtención de componentes y materiales	• Importar o fabricar las piezas era muy difícil, dadas las regulaciones y vigilancia • Fabricación de piezas no requiere infraestructura compleja • Requiere involucramiento de menos personas y menos países que contribuían con piezas
Rapidez en fabricación	• Desarrollo de componentes a velocidad superior • Permite aprender fácilmente mediante ensayo y error, sustituyendo así conocimiento técnico
Planos digitales	• Facilitan transferencia de información • Eliminan necesidad de conocimiento técnico para la fabricación • Los planos pueden conseguirse utilizando un escáner 3d • Permite fabricación de piezas muy reguladas y necesarias para la fabricación de armas nucleares
Reduce capacidad de respuesta	• Requiere involucramiento de menos personas y menos países que contribuyan con piezas, disminuyendo información para la detección por parte de organismos de inteligencia • Reduce la capacidad de las sanciones internacionales, que eran una de las principales herramientas de política exterior encaminadas a la no proliferación

Fuente: Adaptación propia con base en Fey (2017).

o patógenos biológicos potencialmente perjudiciales. Dada la amplia distribución, el bajo costo y el acelerado ritmo del desarrollo de esta tecnología […], su mal uso deliberado o sin intención podría llevar a […] implicaciones de seguridad nacional" (Clapper, 2016, p. 9). La creación a bajo costo proviene de nuevas técnicas como CRISPR, pues mientras otros métodos tienen un costo aproximado de USD 5.000 por cada proceso, en CRISPR dicho valor se reduce hasta USD 30 (Gerstein, 2016a; 2016b). Los impactos de la edición genética y la biología sintética tienen dos formas: directos (deliberados o no) e indirectos.

Un efecto directo y deliberado fue planteado por Wein & Liu (2005) quienes plantean cómo podría desarrollarse un ataque bioterrorista al liberar toxina botulínica en una planta de producción de leche, causando cientos de miles de víctimas. La condición necesaria para que un evento así tuviera lugar, es la consecución de la toxina por parte de los terroristas. La técnica CRISPR está siendo utilizada para realizar modificaciones genéticas a la bacteria que produce la toxina (*Clostridium botulinum*), lo que permite estimular y facilitar la producción de la toxina (Negahdaripour *et al.*, 2017). Otro caso ilustrativo del uso de la biología sintética fue el virus H5N1 de origen aviar, pues, en el 2011, se logró mutar su cepa hasta el punto de hacerla transmisible por vía respiratoria entre mamíferos (Herfst *et al.*, 2012). Así, pues, la biología sintética amplía las capacidades existentes de los Estados en materia biológica, al tiempo que genera capacidades nuevas –edición a bajo costo– para la creación de agentes biológicos que pueden tener consecuencias masivas.

En resumen, la seguridad militar se ve afectada por el surgimiento de capacidades nuevas como los sistemas autónomos, que operan a partir de la combinación de la IA y la robótica, lo que plantea el escenario de las armas autónomas junto con la reducción de costos y riesgos para realizar un ataque, amplía las capacidades existentes de actores estatales y genera nuevas capacidades para los no tradicionales. Segundo, la datificación profundiza las capacidades de vigilancia, además de reducir asimetrías de información entre actores y permitir respuestas inmediatas. Tercero, la impresión 3D y la biología sintética crean capacidades nuevas para actores no tradicionales y amplían capacidades existentes para los Estados.

3.2. Seguridad económica

La seguridad económica internacional considera los asuntos relacionados con los Estados y los individuos. En ese sentido, la perspectiva utilizada en este trabajo es más amplia que la visión tradicional del realismo y el neorrealismo que contemplan la economía exclusivamente como una fuente o un instrumento del poder del Estado (Cable, 1995; Nesadurai, 2006). Los efectos más significativos ocurren en el crecimiento económico, la disrupción en el comercio internacional y los riesgos derivados de la digitalización y una mayor conectividad.

– Crecimiento económico

Las nuevas tecnologías conllevan asimetrías en el crecimiento económico, de modo que permite la redistribución del poder internacional (Drezner, 2019). Las máquinas generan crecimiento económico al incrementar la productividad total de los factores (Romer, 1990), pero hay otro efecto mediante el cual la IA puede generar crecimiento económico: no como un incremento a la productividad total de los factores, sino como un nuevo factor de producción, resultado de una combinación de capital y trabajo. La IA puede replicar actividades laborales (trabajo) a mayor velocidad y escala; puede también, constituir capital físico en la forma de robots. Y a diferencia del capital tradicional, este puede mejorar con el tiempo gracias a las capacidades de auto aprendizaje. El principal impacto económico de esta percepción es incrementar alrededor del 35 por ciento el crecimiento económico en algunas economías avanzadas para el 2035 e incluso más en aquellas que tienen problemas de población envejecida como Japón o los países en desarrollo que no cuentan con trabajadores con la cualificación para desarrollar algunas actividades (Purdy & Daugherty, 2017). Por lo tanto, los impactos de la IA y la robótica en el crecimiento económico pueden ser significativos en el mediano plazo y pueden reforzar las capacidades materiales de los Estados que ya son potencias o contribuir a cerrar la brecha entre aquellos y los países en desarrollo.

– Comercio internacional

El segundo elemento que genera implicaciones en la seguridad económica es la desestabilización global debido al debilitamiento de las alianzas internacionales y los incentivos para la cooperación como consecuencia de la transformación que la impresión 3D y la auto-

matización generan en el comercio global. El comercio internacional existe principalmente porque un país no puede ser eficiente en la producción de todos los bienes que requiere, de modo que cada país se especializa en producir aquellos bienes en los cuales tiene una ventaja relativa. La impresión 3D reduce la ventaja comparativa al centrar la producción en una máquina que tiene un costo de producción similar en cualquier lugar del mundo (WTO, 2013; Abeliansky, Martínez-Zarzoso & Prettner, 2016). Así las cosas, si el costo de fabricar un producto en Estados Unidos es el mismo que en China ¿para qué importarlo? Cabe resaltar que no todos los bienes –por ejemplo, bienes agrícolas– pueden ser fabricados mediante impresión 3D. Por lo tanto, se espera una reducción de hasta el 40% del comercio global de manufacturas en el 2040 (ING, 2017).

¿Cuál es la consecuencia en materia de seguridad internacional? El comercio internacional disminuye los incentivos de los países para atacarse entre sí y al mismo tiempo los aumenta para defenderse unos a otros. Esto se debe a que el beneficio económico que se obtiene del comercio depende del bienestar del otro Estado. Por lo tanto, se generan incentivos para la defensa de los socios comerciales –a través de alianzas militares–, pues se defienden así, indirectamente, los propios beneficios (Martin & Tayer, 2008; Hegre, Oneal & Russett, 2010)[6]. De este modo, el comercio genera una estructura más densa de las redes de cooperación y con ello una mayor estabilidad tanto militar como comercial (Jackson & Nei, 2015). El hecho de que la impresión 3D tenga la capacidad de reducir los flujos de comercio internacional plantea entonces un escenario negativo, pues al reducir el comercio, incrementa la propensión al conflicto. Al igual que con el crecimiento económico, las implicaciones ocurren por la disminución de capacidades de producción por parte de algunos Estados.

– Riesgos de la conectividad y la digitalización

En tercer lugar, el impacto que el internet de las cosas (IoT) tiene sobre la seguridad económica es que contribuye a incrementar la vulnerabilidad en la producción, puesto que incrementa los procesos internos que dependen del IoT y la interdependencia entre empresas e industrias. Además, el potencial económico del IoT se encuentra subutilizado, pues los empresarios todavía utilizan menos del 10 por ciento de los datos que poseen, lo que quiere decir que la interdependencia será mayor en el futuro (Chui, Ganesan & Patel, 2017).

Respecto al primer aspecto, la medición de la producción, el monitoreo del estado de las plantas de producción y las máquinas –para realizar reparación preventiva–, las cadenas de suministro digitales, el uso de robótica, sensores y datos para la produc-

[6] El argumento sostiene que es más costoso iniciar un conflicto con un Estado si se mantiene un elevado nivel de comercio internacional. Esto se debe a que el conflicto destruiría las ganancias del comercio, incrementando así el costo indirecto de la guerra con ese Estado. En modo alguno implica que el comercio impida la guerra.

ción, además de la conexión a internet de los objetos producidos, se realizan cada vez más a través de IoT (Deloitte University Press, 2017). Adicionalmente, en lo que concierne al incremento de la interdependencia, ocurre porque crea redes entre los productores, los consumidores y los productos, que forman parte de un ecosistema digital. Para el 2025, se estima que la producción global basada en IoT alcanzará el 11 por ciento y muchos productos y servicios que se utilicen en el futuro estarán basados en IoT. Todo esto hace que las industrias y las empresas se encuentren más conectadas, pero haciendo sus fronteras más porosas, de modo que la afectación a un sector o a una empresa tiene consecuencias más amplias (Alturi, Dietz & Henke, 2017). El sector agrícola no es ajeno a esta tendencia lo que plantea la cuestión de la afectación de la seguridad alimentaria (Saidu, Usman & Ogedebe, 2015). En otras palabras, el internet de las cosas genera una interdependencia en la economía al conectar distintos actores entre sí, lo que también quiere decir que una irrupción a modo de ataque en las comunicaciones tendría un impacto económico negativo (McKinsey Global Institute [MGI], 2016).

En síntesis, se observa que la seguridad económica se ve transformada por el impacto en el crecimiento económico amplía las amenazas existentes de que los Estados que son pioneros en tecnología incrementen su producción y se amplíe la brecha con los países menos avanzados, lo que a su vez otorga un poder material. En segundo lugar, la reducción del comercio internacional de bienes como consecuencia de la impresión 3D, disminuye los incentivos para mantener las alianzas militares y para evitar los conflictos, pues se reduce la interdependencia económica, creando una nueva amenaza. Por último, la digitalización de la economía y de los procesos productivos por medio del IoT, hace que la exposición a riesgos de ciberataques sea mayor, aumentando capacidades ya existentes para los actores tradicionales y no tradicionales.

3.3. Seguridad societal

La seguridad societal hace referencia a la seguridad de la sociedad considerada en su conjunto. Esencialmente, abarca el tema de las identidades junto con la integridad física, el empleo y el terrorismo (Burgess, 2012; Hama, 2017). Los impactos de las nuevas tecnologías en la seguridad societal se encuentran principalmente en la transformación de la organización social como consecuencia de la reducción de los empleos, el crecimiento de la infraestructura inteligente y la modificación humana.

– Empleos y organización social

Primero, la reducción en el número de empleos (por la automatización) y la dificultad para conseguir uno (por la creciente complejidad de los conocimientos) puede conllevar al descontento social. Un análisis de Frey & Osborne (2013) muestra que el empleo de menos de un tercio de los trabajos actuales se encuentra relativamente seguro, de modo que puede que las máquinas sí destruyan –y no solo reemplacen– empleos. Como sostiene Kaplan (2016, p. 116) "la magnitud y el impacto de la IA […] dependerá de qué tan rápido […] las nuevas

tecnologías facilitarán la automatización de las habilidades de los trabajadores".

En ese sentido, la IA es diferente a las transformaciones tecnológicas previas y el asunto es si el sistema social se puede adaptar usando lecciones del pasado.

> No hay duda de que, en el sistema capitalista moderno, la ocupación es la identidad […] y el dolor y la humillación sentidas por aquellos cuyos trabajos han sido reemplazados es claramente un asunto importante […] no veo una manera fácil de resolver esto. Es una consecuencia inevitable del progreso tecnológico (Mokyr, citado en Rotman, 2017, p. 94).

Lo anterior resulta problemático por varias razones, pues, si las sociedades están inconformes con sus perspectivas y las características del gobierno de turno, "se hará evidente [la capacidad de] sublevarse" (Brynjolfsson & McAfee, 2015, p. 132).

Por lo tanto, la disrupción en el mercado laboral crea una amenaza a la estabilidad social, dado que pone en riesgo los ingresos y la identidad de los individuos. De igual modo, incrementa las capacidades económicas de aquellos Estados que logren desarrollar y aplicar las nuevas tecnologías.

– Infraestructura inteligente

La infraestructura inteligente crea una nueva amenaza para la sociedad: el ataque digital a la infraestructura. Esto ocurre puesto que el internet de las cosas tiene entre sus aplicaciones principales el mantenimiento preventivo, el monitoreo avanzado, los sistemas de vigilancia por video, los sistemas de señalización, la seguridad y gestión de la eficiencia de energía (Fraga, Fernández & Castedo, 2017). Para ilustrar esta cuestión, se toma como caso de estudio el transporte férreo, donde ha surgido el concepto de trenes inteligentes. En este contexto, el IoT permite que la infraestructura férrea esté digitalizada casi en su totalidad (sistema eléctrico, sistema sanitario, puertas, monitoreo de baterías, comunicaciones, velocidad y frenos), además de la automatización o semi-automatización de otras de sus operaciones. En cuanto a la seguridad, el IoT presenta un uso doble, pues al mismo tiempo que monitorea los actos físicos, la prevención de accidentes y los ataques contra la infraestructura, también se hace susceptible a ciberataques, pues al estar conectada, la infraestructura se hace vulnerable. Por lo tanto, "la investigación a futuro relacionada con la seguridad férrea deberá enfocarse en el surgimiento de nuevas ciber-amenazas, [dado que] la automatización […] de los trenes puede convertirse en un gran riesgo potencial" (Fraga, Fernández & Castedo, 2017, p. 28). Las amenazas se amplían, dado que el acceso a la infraestructura puede ser remoto (utilizando internet o sistemas de comunicación); directo (a través de contacto con la infraestructura, por ejemplo, utilizando memorias USB) o localmente (accediendo –sin autorización– a la infraestructura física).

Estas amenazas provienen de distintas fuentes, entre las que se encuentran la infraestructura física (vías, túneles, puentes, intersecciones, interruptores); unidades móviles (locomotoras); estaciones de tren (interiores, exteriores y áreas circundantes); sistemas de control (señalamiento, gestión del tráfico); sistemas y redes de comunicación; sistemas de provisión

de energía y pasajeros (Fraga, Fernández & Castedo, 2017). Ahora bien, similares desafíos surgen para otro tipo de infraestructuras inteligentes en las ciudades, pues al crear un entorno de redes múltiples se pueden bloquear varias funcionalidades de la ciudad (Fantacci & Marabissi, 2016). Asimismo, las redes de suministro de energía también han ingresado en la esfera de las infraestructuras inteligentes, planteando desafíos a una de las infraestructuras fundamentales. No obstante, los avances en protección de infraestructuras –tanto en detección como en reacción– y en prevención de ciberataques se han logrado a partir del uso de sistemas de inteligencia artificial (Wu, Ota, Dong & Li, 2016).

El surgimiento de la infraestructura inteligente crea nuevas capacidades para los actores estatales y no estatales. Dado que permite atacar a distancia la infraestructura crítica (transporte, electricidad, agua, internet), y más aún: permite generar impactos en el mundo físico a través del medio digital.

– Biología sintética

Un tercer impacto a la seguridad societal a escala internacional proviene de la biología sintética. Varias empresas se dedican a identificar cuáles son los genes que determinan o influyen en la inteligencia de los humanos. Buscan incrementar el coeficiente intelectual de cada generación a través de la selección artificial y la fertilización *in vitro* (Bohannon, 2013). Las implicaciones internacionales son claras, como afirma Metzl (2014, párrafo 14): "si China comienza a mejorar su población y Estados Unidos no, podría haber serias repercusiones competitivas". Por ejemplo, "¿qué haría Estados Unidos si supiera que China tiene una iniciativa efectiva de mejora genética humana que le diera a China una ventaja competitiva insuperable en unas cuantas décadas? ¿Estados Unidos no haría nada y aceptaría una potencial pérdida de competitividad, intentaría detener a China por medios individuales o colectivos o igualar a China mejorando su propia población? ¿Qué haría el mundo si actores no estatales […] estuvieran cambiando el código genético de sus seguidores fuera de las jurisdicciones nacionales?" (Metzl, 2014, párrafo 19). De este modo, los asuntos relacionados con la ingeniería genética plantean desafíos para la seguridad internacional, como la desigualdad genética (Simmons, 2008).

En resumen, los impactos de las nuevas tecnologías en la seguridad societal se centran en la organización social y las capacidades económicas, que se redistribuyen en función del desarrollo y aplicación de nuevas tecnologías hacia los actores tradicionales. De igual modo, la vulnerabilidad de la infraestructura representa una amenaza para la sociedad y para la economía, pues los actores tradicionales y no tradicionales obtienen la capacidad de afectar elementos físicos desde el ámbito computacional y digital. Además, surge la cuestión de la edición genética en humanos y las presiones competitivas que esto podría crear en las sociedades, conduciendo incluso a una desigualdad genética.

3.4 Seguridad política

Las transformaciones en el ámbito político se encuentran en los desafíos ante el creciente

volumen de información, que es procesado por sistemas no biológicos. Sin embargo, la disponibilidad de un volumen creciente de datos representa información valiosa para apoyar la toma de decisiones en el ámbito político. La elección de una mejor política es posible gracias al análisis de información histórica e información en tiempo real procesada a través de sistemas de IA. A nivel internacional abre la oportunidad para la verificación del cumplimiento de tratados y compromisos, de modo que permite transparencia y objetividad.

Ahora bien, el principal impacto de los sistemas de IA en la política están en la misma línea que los impactos militares: el uso creciente de algoritmos para la toma de decisiones. A medida que los algoritmos "se vuelvan más autónomos e invisibles, para el público se volverán más difíciles de detectar [así como de] escrutar su imparcialidad" (Janssen & Kuk, 2016, p. 371). Esto es un fenómeno denominado 'algocracia' que se define como un tipo de sistema gubernamental "en el cual los algoritmos son utilizados para recolectar, comparar y organizar los datos sobre los cuales son tomadas las decisiones y para asistir en cómo esos datos son procesados y comunicados a través del sistema de gobierno" (Danaher, 2016, p. 248)[7]. Esto plantea la cuestión de la legitimidad[8] de las políticas, pues si estas son diseñadas con base en la información otorgada por sistemas de IA que pueden ser incomprensibles para el entendimiento humano, la población podría no considerarlas legítimas. De este modo, existe el riesgo de que los humanos puedan resultar "actuando como meros implementadores de juicios basados en algoritmos [o] en algunos casos, los sistemas pueden ser totalmente automatizados" (Danaher, 2016, p. 249). En el ámbito político, los algoritmos limitan la participación y la comprensión humana acerca de decisiones referentes a aspectos que son importantes para la vida humana. De cualquier modo, la amenaza está en marcha y la algocracia representa un desafío para la democracia y los valores políticos contemporáneos (Danaher, 2016). Entonces la sociedad debe enfrentarse a un dilema: mayor eficiencia sin entender cómo opera y sin lograr mayor participación o entendimiento y participación a expensas de la eficiencia. Además, la inteligencia artificial puede ser utilizada para influir en decisiones políticas y en elecciones. Casos como la influencia rusa en las elecciones del 2016 en Estados Unidos evidencian cómo puede ocurrir. Aunque estas actividades se han realizado desde tiempo atrás mediante diferentes mecanismos, la inteligencia artificial y

[7] Durante 2014, en Australia se aprobaron 29 proyectos de ley que aprueban el uso de algoritmos autónomos para tomar decisiones. Los temas abarcan desde control de las exportaciones, pasando por el sistema fiscal hasta el sistema de salud (Elvery, 2017). Por otro lado, a nivel empresarial en Estados Unidos, las decisiones basadas en datos se han triplicado del 2005 al 2010, pasando del 11 al 30% (Brynjolfsson & McElheran, 2017). Esta mayor dependencia de los datos crea la presión para el uso de sistemas de inteligencia artificial, requerida para su procesamiento.

[8] Entendida como el derecho y la aceptación de una autoridad. Se basa principalmente en la creencia en que las acciones del gobierno son apropiadas, transparentes y legales. Para una profundización, véase Hurd (1999).

el aprendizaje automático permiten realizarlo a menor costo y por parte de actores no tradicionales.

En síntesis, las implicaciones en la seguridad política se encuentran en el uso de inteligencia artificial para la toma de decisiones políticas, y la influencia en las elecciones. Frente a lo primero, su funcionamiento puede ser incomprensible para los humanos, lo que plantea una amenaza por la carencia de legitimidad que estas decisiones puedan tener. Por otro lado, actores estatales y no estatales amplían la capacidad de influir en las elecciones y decisiones políticas de otros Estados, utilizando estos mecanismos computacionales. De igual modo, se plantea la cuestión de utilizar tales sistemas para tomar las decisiones políticas, aumentando la eficiencia, pero disminuyendo el entendimiento.

Los resultados anteriores permiten evidenciar que las tecnologías de la cuarta revolución industrial empoderan actores al transformar las capacidades, y permiten impactar el mundo físico a través del ámbito computacional y digital. Por un lado, la facilidad de uso y la reducción del riesgo para quien opera la nueva tecnología hacen que su difusión sea más rápida y tenga una mayor cobertura, pudiendo ser utilizadas por uno o más actores y, de este modo, empoderándolos. Un ejemplo de esto son los Estados que tienen capacidad de desarrollo y acción con VANT militares, mientras los actores no estatales pueden acudir a tecnologías similares reduciendo el costo mediante VANT de uso comercial (Ward, 2017). Otra situación surge de la biología sintética, pues permite desarrollar procesos fácilmente en laboratorios de menor envergadura y con personas con menor preparación en edición genética (Ledford, 2010; Garret, 2013). Otro ejemplo es la impresión 3D, la cual empodera desde individuos a grupos, permitiendo fabricación de armas e incluso facilitar la fabricación de piezas de armas de destrucción masiva (Fey, 2017). De modo que puede que la coalición 'híbrida' entre actores estatales y no estatales sea cada vez más necesaria para actuar en la arena internacional (Smith, 2016). Con esto no se quiere decir que todos los actores tendrán la misma importancia y las mismas capacidades; únicamente se pretende mostrar que los Estados están interactuando con mayor frecuencia con actores no tradicionales.

Por otro lado, hay una brecha entre la percepción que se tiene actualmente de lo que representan los ciberataques, pues no se enfocan solo en la información, sino que están aumentando gradualmente la capacidad de afectar el mundo físico. El hecho que internet se haga ubicuo y esté presente en los objetos, además de la conexión de la infraestructura, incrementa su vulnerabilidad y los ataques sin necesidad de elementos físicos (Greenberg, 2017). No obstante, este tipo de ataques digitales, aunque tienen un mayor poder de afectación, tienden a disminuir la letalidad de los ataques, pues se afectan objetos y datos, pero cada vez menos la vida de las personas (Rid, 2013; Goodman, 2015). Así, pues, la disminución del riesgo físico del atacante y la mayor accesibilidad a ciertas armas incrementa la propensión a los ataques y al conflicto (NIC, 2012). Pero estos actores pueden concentrarse y generar una agregación a través de redes que les permitan desafiar a actores como los Estados.

4. CONCLUSIONES

La cuarta revolución industrial genera impactos en la seguridad internacional a través de la creación de nuevas amenazas, el empoderamiento de actores –incluidos los no estatales– otorgándoles nuevas capacidades (innovación disruptiva) y ampliando las existentes (innovación sostenida). En la dimensión militar, la inteligencia artificial y la robótica disminuyen costos y riesgos para el atacante, ampliando así las capacidades existentes para actores estatales y no estatales. Además, la impresión 3D y la biología sintética crean la capacidad para lograr armas de destrucción masiva. En la dimensión económica, el uso de tecnologías supone asimetrías en el crecimiento económico, ampliando las brechas y otorgando así un mayor poder a los ganadores. Adicionalmente, la interdependencia económica global se ve afecta por la reducción de flujos de mercancías e inversión como consecuencia de la impresión 3D. Por último, el internet de las cosas conecta a internet los medios de producción, haciéndolos vulnerables, lo que crea una capacidad nueva para actores tradicionales y no tradicionales.

Frente a la dimensión social, la vulnerabilidad de la infraestructura aumenta al estar conectada mediante internet de las cosas y esta, a su vez, permite impactos físicos a través de mecanismos digitales, disminuyendo los costos y los riesgos para quien genera los ataques, es decir, crea nuevas capacidades para los actores internacionales. Por otro lado, la edición genética crea capacidades nuevas para actores tradicionales y no tradicionales, además de crear incentivos para el dilema de seguridad. En la dimensión política, se aumentan las capacidades existentes de los actores para influir en las elecciones y las decisiones políticas. Estos resultados evidencian que la cuarta revolución industrial expande la seguridad internacional, expande horizontalmente al profundizar la amenaza que supone el ámbito digital y verticalmente al modificar las capacidades de los actores no estatales y los individuos.

Tres temas de investigación a futuro surgen como consecuencia de los resultados de este trabajo. Primero, las limitaciones de la democracia. La tecnología requiere conversaciones nacionales e internacionales amplias para definir cómo las sociedades afrontan el cambio, al tiempo que involucra temas técnicos y éticos. La democracia deliberativa presenta altos costos de oportunidad frente a otros sistemas políticos que tienen la ventaja de centralizar sus decisiones y pueden explotar con mayor facilidad los beneficios de las nuevas tecnologías (Smith, 2016). Segundo, los fundamentos del poder en las relaciones internacionales. En la actualidad el poder económico ya no se transfiere tan fácilmente

[9] Dada la complejidad de la tecnología moderna, desarrollar capacidades militares requiere capacidades de investigación y desarrollo lo cual no se logra únicamente con capacidades económicas (Brooks & Wohlforth, 2016). Por ejemplo, un Estado cuya riqueza provenga de la exportación de recursos minerales, tendrá las capacidades económicas, pero no necesariamente cuenta con el *know-how* y las capacidades tecnológicas necesarias para desarrollar capacidades militares avanzadas.

en capacidades militares[9], pues estas ahora dependen en gran medida de la tecnología y el conocimiento disponible en cada país. En otras palabras, no basta con tener los recursos económicos, hay que saber cómo invertirlos (Brooks & Wohlforth, 2016). Aunque los factores tradicionales de poder (militar y económico) continuarán siendo relevantes, la cuarta revolución industrial modifica la producción económica y las capacidades militares, haciéndolas más dependientes de la tecnología. El poder está fundamentado en la innovación dado que permite desarrollar la tecnología, y así, las capacidades militares y económicas. Por lo tanto, la geotecnología surge, junto a la geopolítica y la geoeconomía, como fundamento del poder y la seguridad en el escenario global[10]. Tercero, el enfoque de la disciplina de las relaciones internacionales. La transformación que genera la cuarta revolución internacional en la seguridad internacional hace que la distinción entre esta disciplina y otras no solo sea más borrosa, sino que además sea un obstáculo para su estudio. Se resaltan las implicaciones de la biología evolutiva, las ciencias de la complejidad, la ciencia de redes y los estudios de ciencia y tecnología[11], pues las relaciones internacionales son un sistema complejo adaptativo y abierto que requiere de nuevas aproximaciones, aunque en ocasiones se crea que son simples hechos de ciencia ficción los que generan las nuevas tecnologías.

La cuarta revolución industrial, por su carácter digital, permite que los ataques sean más propensos (por la facilidad de acceder a las tecnologías), pero menos letales (porque en su mayoría ocurren en el ámbito digital, y los impactos físicos se dan en objetos e infraestructura). Atacar la infraestructura sanitaria de una megaciudad es sin duda catastrófico, pero no es letal. De esta manera, dada la propensión a los ataques, la frontera entre guerra y paz se hace borrosa y, debido a la diversidad de actores, la diferencia entre combatientes y no combatientes tiene la misma tendencia. En un mundo en el cual la seguridad se fundamenta en la información y las tecnologías, es necesario preguntarse: ¿qué es violencia y qué es seguridad en el mundo digital?, ¿es el ciberespacio otra dimensión de la seguridad internacional?, ¿deberían ser los datos también un objeto de referencia de la seguridad, así como lo han sido los Estados, y más recientemente, los individuos?

---

[10] "La geotecnología enfatiza el rol de la tecnología en la formación del orden global al examinar la rápida difusión de la innovación [y] cómo diversos actores en el sistema se basan en la tecnología para aumentar su propio poder e influencia […]. Al elevar la tecnología al nivel del poder económico y militar como un factor de cambio global, el enfoque de geotecnología busca complementar, no reemplazar, la geopolítica y la geoeconomía" (Khanna, 2014, p. 56).

[11] Al respecto, Watson (2017), muestra cómo el avance en el conocimiento ha sido posible por la tendencia a la convergencia entre las diferentes disciplinas, lo que cada vez conduce a más hallazgos que, de otra manera, serían imposibles de lograr. Como lo señala Weiss (2015), la ausencia de otras disciplinas, en particular la ciencia y la tecnología, es notoria en los análisis de relaciones internacionales.

REFERENCIAS

Abeliansky, A. L.; Martínez-Zarzoso, I. & Prettner, M. (2016). The impact of 3D printing on trade and FDI. *Beiträge zur Jahrestagung des Vereins für Socialpolitik 2016: Demographischer Wandel - Session: International Trade and Development, No. A19-V1*. Disponible en http://hdl.handle.net/10419/145479

Agrawal, A.; Gans, J. & Goldfarb, A. (2019) *Prediction Machines: The Simple Economics of Artificial Intelligence*. Boston, United States: Harvard Business Review Press.

Alturi, V.; Dietz, M. & Henke, N. (2017). Competing in a world of sectors without borders. *McKinsey Quarterly*, *3*, 32-47.

Autor, D. H. (2014). Polanyi's Paradox and the Shape of Employment Growth. *NBER Working Paper No. 20485*. Disponible en http://www.nber.org/papers/w20485.pdf

Autor, D. H. (2015). Why Are There Still So Many Jobs? The History and Future of Workplace Automation. *Journal of Economic Perspectives*, *9*(3), 3-30. DOI: 10.1257/jep.29.3.3

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, *23*, 5-26

Bjola, C. & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. New York, United States: Routledge.

Bohannon, J. (2013). Why Are Some People So Smart? The Answer Could Spawn a Generation of Superbabies. *Wired*. Disponible en https://www.wired.com

Brooks, S. G. & Wohlforth, W. C. (2016). The Rise and Fall of the Great Powers in the Twenty-first Century. *International Security*, *40*(3), 7-53.

Browning, C. S. (2013). *International Security: A Very Short Introduction*. New York, United States: Oxford University Press.

Brynjolfsson, E. & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, United States: W. W. Norton & Company.

Brynjolfsson, E. & McAfee, A. (2015). ¿Correrán los humanos la misma suerte que los caballos? *Foreign Affairs Latinoamérica*, 15(4), 127-133.

Brynjolfsson, E. & McElheran, K. (2017). The Rapid Adoption of Data-Driven Decision-Making. *American Economic Review*, 106(5), 133-139. DOI: 10.1257/aer.p20161016.

Burgess, J. P. (2012). The Societal Impact of Security Research. Peace Research Institute Oslo, *PRIO Policiy Brief* No. 09/2012. Disponible en http://file.prio.no/

Buzan, B. (1983). *People, States & Fear: The National Security Problem in International Relations*. Boulder, United States: Lynne Reiner.

Buzan, B. & Lawson, G. (2015). *The Global Transformation: History, Modernity and the Making of International Relations*. Cambridge, United Kingdom: Cambridge University Press.

Buzan, B.; Weaver, O. & de Wilde, J. (1997). *Security: A new framework for analysis*. Boulder, United States: Lynne Rienner.

Cable, V. (1995). What is international economic security? *International Affairs*, *71*(2), 305-324. DOI: 10.2307/2623436.

Christensen Raynor, M. & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review*, *93*(12), 44-53.

Chui, M.; Ganesan, V. & Patel, M. (2017). Taking the pulse of enterprise IoT. *McKinsey & Company*. Disponible en https://www.mckinsey.com/

Clapper, J. R. (09/02/2016). Worldwide Threat Assesment of the US Intelligence Community. Disponible en https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Collins, A. (2007). *Contemporary Security Studies*. New York, United States: Oxford University Press.

Cronin, A. K. (2020). *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. New York, United States: Oxford University Press.

Cummings, M. L.; Roff, H. M.; Cukier, K.; Parakilas, J. & Bryce, H. (2018). Artificial Intelligence and International Affairs, *Chatham House Report*. Disponible en www.chathamhouse.org/

Danaher, J. (2016). The Threat of Algocracy: Reality, Resistance and Accommodation. *Philosophy & Technology*, *29*(3), 245-268.

Deloitte University Press. (2017). *Industry 4.0 and cybersecurity*. *Deloitte series on digital manufacturing*. Disponible en https://dupress.deloitte.com

Department of Defense (DoD). (2016). Department of Defense Additive Manufacturing Roadmap. Final Report. Disponible en https://www.americamakes.us/images/publicdocs/DoD%20AM%20Roadmap%20Final%20Report.pdf

Drezner, D. (2019). Technological change and international relations. *International Relations*, 33(2), 286-303. DOI: 10.1177/0047117819834629.

Elvery, S. (2017). How algorithms make important government decisions — and how that affects you. *ABC News*. Disponible en http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858

Executive Office of the President. (2016). Artificial Intelligence, Automation, and the Economy. Disponible en https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy

Fantacci, R. & Marabissi, D. (2016). Cognitive Spectrum Sharing: An Enabling Wireless Communication Technology for a Wide Use of Smart Systems. *Future Internet*, *8*(2), 23. DOI: 10.3390/fi8020023.

Fey, M. (2017). 3D Printing and International Security. Peace Research Institute Frankfurt, *PRIF Report* No. 144.

Fraga, P.; Fernández, T. & Castedo, L. (2017). Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways. *Sensors*, 17(6), 1457. DOI: 10.3390/s17061457.

Fraga-Lamas, P.; Fernández, T. M.; Suárez, M.; Castedo, L. & González, M. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors*, *16*(10), 1644. DOI: 10.3390/s16101644.

Franke, U. E. (2016). The Global Diffusion of Unmanned Aerial Vehicles (UAVs), or 'Drones'. En Aaronson, M.; Aslam, W.; Dyson, T. & Rauxloh, R. (Eds.), *Precision Strike Warfare and International Intervention: Strategic, Ethico-legal, and Decisional Implications*. New York, United States: Routledge.

Frasson-Quenoz, F. (2014). *Autores y teorías de relaciones internacionales: Una cartografía*. Bogotá, Colombia: Universidad Externado de Colombia.

Frey, C. B. (2019). *The Technology Trap: Capital, Labor, and Power in the Age of Automation*. New Jersey, United States: Princeton University Press.

Frey, C. B. & Osborne, M. A. (2013). *The future of employment: How susceptible are jobs to computerization?* Working Paper, Oxford Martin School, Oxford University. Disponible en http://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf

Garret, L. (2013). Biology's Brave New World. *Foreign Affairs*, 92(6), 28-46.

Gershenfeld, N. (2013). Cómo hacer (casi) cualquier cosa: la revolución de la fabricación digital. *Foreign Affairs Latinoamérica*, 91(6), 140-152.

Gerstein, D. M. (2016a). How genetic editing became a national security threat. *Bulletin of the Atomic Scientists*. Disponible en http://thebulletin.org/how-genetic-editing-became-national-security-threat9362

Gerstein, D. M. (2016b). Can the bioweapons convention survive Crispr? *Bulletin of the Atomic Scientists*. Disponible en http://thebulletin.org/can-bioweapons-convention-survive-crispr9679

Goodman, M. (2015). *Los delitos del futuro*. Barcelona, España: Ariel.

Greenberg, A. (2017). How an entire nation became Russia's test lab for cyberwar. *Wired*. Disponible en https://www.wired.com/story/russian-hackers-attack-ukraine/

Greg, A. & Chan, T. (2017). Artificial Intelligence and National Security. *Belfer Center for Science and International Affairs, Harvard Kennedy School*. Disponible en https://www.belfercenter.org/

Hama, H. H. (2017). State Security, Societal Security, and Human Security. *Jadavpur Journal of International Relations*, 21(1), 1-19. DOI: 10.1177/0973598417706591.

Harari, Y. N. (2016). *Homo Deus: Breve historia del mañana.* Bogotá, Colombia: Debate.

Hegre, H.; Oneal, J. R. y Russett, B. (2010). Trade does promote peace: new simultaneous estimates of the reciprocal effects of trade and conflict. *Journal of Peace Research*, 47(6), 763-774. DOI: 10.1177/0022343310385995.

Herfst, S.; Schrawen, E. J. A.; Linster, M.; Chutinimitkul, S.; de Wit, E.; Munster, V. J., […] Fouchier, R. A. (2012). Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets. *Science*, 336(6088), 1534-1541. DOI: 10.1126/science.1213362.

Hooker, J. & Kim, T. W. (2019). Ethical Implications of the Fourth Industrial Revolution for Business and Society. En Wasieleski, D. M. & Weber, J. (Eds.), *Business Ethics* (pp. 35-63). Bingley, United Kingdom: Emerald Publishing Limited. DOI: 10.1108/S2514-175920190000003002.

Hurd, I. (1999). Legitimacy and Authority in International Politics. *International Organization*, 53(2), 379-408.

ING. (2017). 3D printing: a threat to global trade. *ING Economic and Financial Analysis*. Disponible en https://www.ingwb.com/media/2088633/3d-printing-report-031017.pdf

Jackson, M. O. & Nei, S. (2015). Networks of military alliances, wars, and international trade. *Proceedings of the National Academy of Sciences*, *112*(50), 15277–15284. DOI: 10.1073/pnas.1520970112.

Janssen, M. & Kuk, G. (2016). The challenges and limits of big data algorithms in technocratic governance. *Government Information Quarterly*, 33(3), 371-377. DOI: 10.1016/j.giq.2016.08.011.

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, 35(2), 147-169. DOI: 10.1080/14751798.2019.1600800.

Kaplan, J. (2016). *Artificial Intelligence: What Everyone Needs to Know*. New York: Oxford University Press.

Khanna, P. (2014). Geotechnology and Global Change. *Global Policy*, 5(1), 54. DOI: 10.1111/1758-5899.12117.

Kleinman, A. (23/05/2013). 3D printed bullets exist, and they are terrifyingly easy to make. *The*

Huffington Post. Disponible en http://www.huffingtonpost.com/2013/05/23/3d-printed-bullets_n_3322370.html

Kosal, M. E. (2020). *Disruptive and Game Changing Technologies in Modern Warfare*. Switzerland: Springer Nature.

Kreps, S. E. (2016). *Drones: What Everyone Needs to Know*. New York, United States: Oxford University Press.

Kroenig, M. & Volpe, T. (2015). 3-D Printing the Bomb? The Nuclear Nonproliferation Challenge. *The Washington Quarterly*, 38(3), 7-19. DOI: 10.1080/0163660X.2015.1099022.

Ledford, H. (2010). Garage biotech: Life hackers. *Nature*, 437, 650-652. DOI: 10.1038/467650a.

Lodgaard, S. (1991). Vertical and Horizontal Proliferation in the Middle East/Persian Gulf. *Bulletin of Peace Proposals*, 22(1), 3-10.

Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures*, *90*, 46-60. DOI: 10.1016/j.futures.2017.03.006.

Martin, P. y Tayer, T. (2008). Make Trade Not War? *Review of Economic Studies*, *75*(3), 865-900. DOI: 10.1111/j.1467-937X.2008.00492.x.

McAfee, A. & Brynjolfsson, E. (2016). Human Work in the Robotic Future. *Foreign Affairs*, 95(4), 139-150.

McCafferty, S. (2016). Military Robots: The Fighting Force of The Future. Monograph, School of Advanced Military Studies, United States Army Command and General Staff College. Fort Leavenworth, United States.

McKinsey Global Institute [MGI]. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy. *McKinsey & Company*. Disponible en https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies

Metzl, J. F. (2014). The Genetics Epidemic. *Foreign Affairs*. Disponible en https://www.foreignaffairs.com/articles/united-states/2014-10-10/genetics-epidemic

Mutimer, D. (2007). Critical Security Studies: A Schismatic History. En A. Collins (Ed.), *Contemporary Security* Studies (pp. 53-74). New York, United States: Oxford University Press.

Naím, M. (2016). *El fin del poder*. Bogotá, Colombia: Debate.

National Intelligence Council (NIC). (2012). *Alternative Wolrds: Global Trends 2030*. Publication NIC 2012-001.

Negahdaripour, M.; Nezafat, N.; Hajighahramani, N.; Rahmatabadi, S. S. & Ghasemi, Y. (2017). Investigating CRISPR-Cas systems in Clostridium Botulinum via bioinformatics tools. *Infection, Genetics and Evolution*, 54, 355-373. DOI: 10.1016/j.meegid.2017.06.027.

Nesadurai, H. E. S. (2004). Introduction: economic security, globalization and governance. *The Pacific Review*, *17*(4), 459-484. DOI: 10.1080/0951274042000326023.

New America Foundation. (2017). 5. Non-State Actors with Drone Capabilities. *World of Drones in-depth report*. Disponible en https://www.newamerica.org/

Oh, H.; Kim, S.; Shin, H-S.; Tsourdos, A. & White, B. A. (2014). Behaviour recognition of ground vehicle using airborne monitoring of unmanned aerial vehicles. *International Journal of Systems Science*, 45(12), 2499-2514. DOI: 10.1080/00207721.2013.772677.

Patterson, D. R. (2017). Defeating the threat of small unmanned aerial systems. *Air & Space Power Journal*, *31*(1), 15-25.

Price Waterhouse Coopers [PWC]. (2018). *A drone's eye view*. PWC-Agoria Report. Recuperado de: https://www.pwc.be/

Purdy, M. & Daugherty, P. (2017). Why Artificial Intelligence is the Future of Growth. *Accenture Report*. Disponible en https://www.accenture.com/us-en/insight-artificial-intelligence-future-growth

Puyvelde, D. V.; Coulthart, S. & Hossain, M. S. (2017). Beyond the buzzword: big data and national security decision-making. *International Affairs*, 93(6), 1397-1416. DOI: 10.1093/ia/iix184.

Raytheon. (2015). To print a missile. *Raytheon Company*. Disponible en http://www.raytheon.com/news/feature/3d_printing.html

Rid, T. (2013). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs*, 92(6), 77-87.

Robertson, A. (2013). A 3D-printed gun can still explode but making an AK-47 is easier than you think. *The Verge*. Disponible en https://www.theverge.com/2013/5/24/4362236/watch-a-3d-pistol-explosion-and-ak-47-kit-making

Romer, P. (1990). Endogenous Technological Change. *Journal of Political Economy*, 98(5), 71-102.

Rothschild, E. (1995). What is Security? *Daedalus*, 124(3), 53-98.

Rotman, D. (2017). The Relentless Pace of Automation. *MIT Technology Review*, 120(2), 92-95.

Saidu, C. I.; Usman A, S. & Ogedebe, P. (2015). Internet of Things: Impact on Economy. *British Journal of Mathematics & Computer Science*, 7(4), 241-251. DOI: 10.9734/BJMCS/2015/14742.

Scharre, P. (2018). *Army of none: autonomous weapons and the future of war*. New York, United States: W. W. Norton & Company.

Schwab, K. (2016). *The Fourth Industrial Revolution*. Geneva, Switzerland: World Economic Forum.

Simmons, D. (2008). Genetic inequality: Human genetic engineering. *Nature Education*, *1*(1), 173.

Singer, P. W. (2009). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York, United States: Penguin Group.

Smith, A. (2016). Technology and International Security. En Noonan, N. C. & V. Nadkami (eds.), *Challenge and Change: Global Threats and the State in Twenty-first Century International Politics* (pp. 165-193). New York, United States: Palgrave Macmillan US.

Tinnirello, M. (2018). Offensive Realism and the Insecure Structure of the International System: Artificial Intelligence and Global Hegemony. En Yampolsky, R. V. (Ed.), *Artificial Intelligence Safety and Security* (pp. 339-356). Boca Raton, United States: CRC Press- Taylor & Francis Group.

Walther, G. (2015). Printing Insecurity? The Security Implications of 3D-Printing of Weapons. *Science and Engineering Ethics*, 21(6), 1435-1445. DOI: 10.1007/s11948-014-9617-x.

Ward, A. (2017). Guess who has drones now? ISIS. *Vox*. Disponible en https://www.vox.com/

Watson, P. (2017). *Convergencias*. Bogotá, Colombia: Crítica.

Weaver, O. (1995). Securitization and Desecuritization. En Lipschutz, R. D. (Ed.), *On Security* (pp. 46-87). New York, United States: Columbia University Press.

Wein, L. M. & Liu, Y. (2005). Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. *Proceedings of the National Academy of Sciences*, *102*(28), 9984-9989. DOI: 10.1073/pnas.0408526102.

Weiss, C. (2015). How Do Science and Technology Affect International Affairs? *Minerva*, 53(4), 411-430.

World Trade Organization (WTO). (2013). *World Trade Report 2013: Factors shaping the future of world trade*. Geneve, Switzerland: World Trade Organization.

Wu, J.; Ota, K.; Dong, M. & Li, C. (2016). A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities. *IEEE Access*, *4*, 416-424. DOI: 10.1109/ACCESS.2016.2517321.