ESTUDIOS

DISERTACIONES

Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional

ISSN: 1856-9536

Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804

Volumen 16, Número 2 / Julio-diciembre 2023

Versión PDF para imprimir desde

http://revistas.urosario.edu.co/index.php/disertaciones

Para citar este artículo: Flores-Vivar, J. M., Gómez-de-Ágreda, Á., & Gómez-López, J. (2023). Taxonomía de la inteligencia artificial en el entorno cognitivo de los conflictos. *Anuario Electrónico de Estudios en Comunicación Social "Disertaciones"*, *16*(2). https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804

TAXONOMÍA DE LA INTELIGENCIA ARTIFICIAL EN EL ENTORNO COGNITIVO DE LOS CONFLICTOS

Taxonomy of Artificial Intelligence in the Cognitive Conflict Environment

Taxonomia da inteligência artificial no ambiente cognitivo de conflitos

Jesús Miguel Flores-Vivar, Universidad Complutense de Madrid (España).
jmflores@ucm.es
Ángel Gómez-de-Ágreda, Ejército del Aire-Ministerio de Defensa (España).
agdeagreda@gmail.com
Jacinto Gómez-López, Universidad Complutense de Madrid (España).
jacintog@ucm.es

Recibido: 28 de diciembre de 2022
Aprobado: 21 de marzo de 2023
Fecha de prepublicación: 23 de mayo de 2023

RESUMEN

El artículo aborda el estado del arte y análisis del paradigma de inteligencia artificial (IA) aplicada a usos bélicos. Se reflexiona cómo los conflictos contemporáneos se libran en muy buena parte fuera de los campos de batalla, incluso en ámbitos no físicos, como el cibernético y el cognitivo. En estos dos entornos se da un uso no menos intenso de la IA con la misma finalidad de alterar la voluntad de los adversarios, valiéndose fundamentalmente de herramientas de influencia y desinformación. La metodología utilizada se basa en la revisión bibliográfica y análisis de documentos elaborados por expertos e informes de instituciones dedicadas al tratamiento de la ciberseguridad, defensa y acciones bélicas en los países desarrollados. Se propone una taxonomía de las aplicaciones

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

bélicas y maliciosas de la IA que prescinde de las características tecnológicas de esta para centrarse en su aplicación operacional. El resultado no es un conjunto cerrado de opciones, sino que se ramifica en numerosas alternativas susceptibles de ser desarrolladas en otros trabajos. La conclusión principal que se alcanza es que los países deben tener en cuenta el potencial de la IA para desarrollar acciones tácticas y estratégicas, preparándose para escenarios no convencionales.

Palabras clave: inteligencia-artificial; seguridad; defensa; guerra.

ABSTRACT

The article focuses on the state of the art and analysis of the artificial intelligence (AI) paradigm as applied to warfare. It shows how contemporary wars are largely fought outside the battlefields, even in non-physical environments, including cybernetic and cognitive ones. In these two environments, there is intense use of AI to alter the will of adversaries, mainly through influence and disinformation tools. The methodology used is based on a literature review and analysis of documents prepared by experts and reports from institutions dedicated to treating cybersecurity, defense, and warfare in developed countries. Here, we propose a taxonomy of warfare and malicious applications of AI that dispenses with the technological characteristics of AI to focus on its operational application. This does not result in a closed set of options but branches into numerous alternatives that can be developed in other works. The primary conclusion is that countries should consider the potential of AI to develop tactical and strategic actions and prepare for unconventional scenarios.

Keywords: Artificial intelligence; security; defense; warfare.

RESUMO

O artigo aborda o estado da arte e análise do paradigma da inteligência artificial (IA) aplicado a usos bélicos. Reflete sobre como os conflitos contemporâneos são travados em grande medida fora dos campos de batalha, mesmo em campos não físicos, como o cibernético e o cognitivo. Nestes dois ambientes, ocorre um uso não menos intenso de IA com o mesmo objetivo de alterar a vontade dos adversários, principalmente por meio de ferramentas de influência e desinformação. A metodologia utilizada baseia-se na revisão bibliográfica e análise de documentos elaborados por especialistas e relatórios de instituições dedicadas ao tratamento de cibersegurança, defesa e ações de guerra em países desenvolvidos. É proposta uma taxonomia das aplicações bélicas e maliciosas da IA que desconsidera suas características tecnológicas para focar em sua aplicação operacional. O resultado não é um conjunto fechado de opções, mas ramificações em inúmeras alternativas que podem ser desenvolvidas em outros trabalhos. A principal conclusão a que se chega é que os países devem levar em consideração o potencial da inteligência artificial para desenvolver ações táticas e estratégicas, preparando-se para cenários não convencionais.

Palavras-chave: inteligência artificial; segurança; defesa; guerra.

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

La importancia de las percepciones en la configuración de la opinión pública y en las decisiones políticas no es nueva (Leonardo-Oviedo, 2004). La racionalidad requiere la capacidad de dar sentido a lo que se percibe, pero la libertad exige que ese sentido esté basado en percepciones apoyadas en la realidad. Umberto Eco, preocupado por el fenómeno de la desinformación, hacía un llamamiento a la responsabilidad de la prensa en el último artículo que publicó en *L´Expresso*. No puede existir libertad sin verdad, por cuanto las elecciones se basarían en criterios espurios. Don Miguel de Unamuno hacía referencia a este aspecto en su famosa divisa inmortalizada en la fachada de su Casa Museo, aneja a la de la Universidad de Salamanca: "Primero la verdad que la paz".

La configuración de los relatos y su capacidad de influencia han estado siempre condicionadas por la tecnología disponible para elaborarlos y difundirlos. Así, las distintas etapas tecnológicas de la humanidad vienen marcadas por la materia prima que se dominaba (piedra, bronce, hierro…). También las formas de generar y transmitir los relatos han condicionado los modos de influencia. La tradición oral, la invención de la escritura o, posteriormente, de la imprenta han propiciado cambios geopolíticos intensos. En muchos casos, ello ha implicado la desaparición de viejos modos de gobernanza y el surgimiento de otros nuevos. La tecnología que ha producido esos cambios muestra la emergencia de nuevos conceptos que escapan al tradicional conflicto armado (Gómez-López, 2019).

Las técnicas asociadas con lo que se viene llamando inteligencia artificial (IA), junto con el incremento exponencial en la capacidad de procesamiento, se están aplicando a la práctica totalidad de las actividades humanas. Comprenden sus vertientes psicológicas, sociológicas y políticas, incluida en esta la actividad bélica. Otro tanto puede decirse de los aspectos éticos y reguladores de los sistemas de IA (Flores-Vivar & García-Peñalvo, 2023), cuyos expertos deberán ejercer su labor sobre el concepto de la IA y no de forma separada sobre cada uno de sus cambiantes usos. Para Josef Baker-Brunnbauer (2023), los sistemas de IA en rápido desarrollo tienen un tremendo potencial para cambiar por igual varios dominios y ejercer una influencia considerable en sociedades y organizaciones. Más que una mera disciplina técnica, la IA requiere la interacción entre varias profesiones. Para Ana Ayerbe (2020), los grandes avances en IA que se están dando han sido posibles gracias al mayor conocimiento sobre el funcionamiento del cerebro adquirido en los últimos años, los avances en microelectrónica, el aumento de la potencia de computación y la posibilidad de acceder a grandes cantidades de datos y la conexión ubicua entre sistemas.

Por ello, si bien la naturaleza de la guerra no cambia sustancialmente con su empleo, sí puede afirmarse que los límites que definen su esencia se vuelven más borrosos e indefinidos. Tanto las tecnologías como las técnicas bélicas las emplean con fines maliciosos los criminales en tiempo de paz, y las propias de estos en operaciones de guerra. Por tanto, el impacto de la IA va mucho más allá del mediático empleo de los medios no tripulados. Su acción afecta también a factores estratégicos como la disuasión y la probabilidad de que se produzca una escalada no intencionada en las hostilidades (Johnson, 2020).

Las operaciones de influencia, como otras muchas, se extienden a lo que se ha denominado la zona gris, en la que las agresiones se mantienen por debajo del umbral que detonaría una respuesta por parte del adversario (Calvo-Albero, 2020). Por lo tanto, tienen lugar en tiempo de "no guerra". Este escenario busca la degradación de las capacidades del adversario, sin distinción entre las militares y las civiles (Tschopp, 2019).

La presencia de la IA puede detectarse fácilmente en los medios cinéticos empleados en los últimos conflictos. En estos predomina el empleo de plataformas (vehículos) no tripuladas y vectores (munición) dotados de un cada vez mayor grado de autonomía. Esta presencia se percibe también en las cada vez más frecuentes operaciones

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

"en enjambre", con plataformas coordinadas mediante algoritmos. El legislador, si bien a un ritmo mucho más pausado —como es el preceptivo— y con las lógicas limitaciones propias del derecho internacional, lleva años acometiendo intentos de regulación de la autonomía de las armas cinéticas.

Sin embargo, tecnologías no letales basadas en principios muy similares tienen también un gran impacto en el desarrollo del conflicto, en su génesis y en su justificación, sin que reciban una atención ni cuidado equivalentes (Scharre, 2019). La letalidad confiere un sentido de urgencia y de gravedad a la aplicación de la IA a sistemas robóticos físicos armados. Esta criticidad no está presente en sistemas robóticos virtuales (como los *chatbots*), cuyas propiedades no están definidas como armas (Gómez-de-Ágreda & Feijoo, 2021).

La creciente corporeización de los dispositivos digitales introduce nuevos condicionantes (Aguado, 2020), no ya por la naturaleza de las tecnologías implicadas, sino por el modo de empleo que se hace de ellas. Son dispositivos que pasan a formar parte de nuestra indumentaria, que nos acompañan en todo momento. Los teléfonos móviles y demás equipos incorporan sensores capaces de complementar nuestros sentidos naturales, y aplicaciones y programas que interpretan las percepciones obtenidas tanto por los sensores artificiales como por los sentidos naturales (Aguado et al., 2013). De este modo, la interpretación de una parte importante de la realidad se externaliza en estos aparatos y da lugar a insumos cognitivos potencialmente sesgados que alteran nuestra interpretación de la realidad (Boyer, 2018).

La IA está lista para desatar la próxima ola de disrupción digital, y las instituciones y empresas deben prepararse ahora (Bughin et al., 2017). Es evidente que ya vemos beneficios en la vida real para algunas empresas de adopción temprana —como la industria armamentística y de defensa—, por lo que es más urgente que nunca que otras aceleren sus transformaciones digitales. Para los investigadores, los hallazgos en la IA se centran en cinco sistemas:

- Robótica y vehículos autónomos.
- Visión por computador.
- Lenguaje.
- Agentes virtuales.
- Aprendizaje automático, que incluye el aprendizaje profundo (*deep learning*) y sustenta muchos avances recientes en otras tecnologías de IA.

La aplicación de técnicas de *machine learning* y *deep learning* permite ya la generación de contenidos sintéticos altamente verosímiles capaces de desvirtuar la realidad percibida de forma mediada a través de determinados dispositivos (Barnes & Barraclough, 2019; Bonfanti, 2020). En febrero de 2019, Gartner (2018) publicó ya su primer informe sobre el aprendizaje automático (*machine learning*) antagónico y advirtió que "los líderes de aplicaciones deben anticipar y prepararse para mitigar los riesgos potenciales de corrupción de datos, robo de modelos y muestras antagónicas". Si bien estas tecnologías requieren todavía grandes inversiones y plazos considerables para la elaboración de los contenidos, siguen siendo mucho más económicas que otras formas de actuación bélica modernas (Chesney & Citron, 2018). Incorporan, además, ventajas asociadas con la discreción y con la posibilidad de negación de autoría, que resultan especialmente útiles en estos ámbitos. Su misma sofisticación contribuye, casi como las armas nucleares, a devolver a los Estados el monopolio del uso de un determinado tipo de fuerza (Boulanin, 2018).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

A pesar de todo, la prevalencia de los llamados *cheap fakes* (Paris & Donovan, 2019; Schick, 2020), alteraciones poco sofisticadas de imágenes o video, y de los *memes* (Helmus, 2022) demuestra que el factor determinante no es el estudio de la tecnología (ingeniería), sino el de las vulnerabilidades cognitivas del objetivo (sociología y psicología). Uno de los principales cambios que introduce la aplicación de la IA como herramienta de manipulación de las percepciones y las emociones tiene que ver con la mayor comprensión que su estudio ha proporcionado sobre los mecanismos cognitivos naturales. El estudio de las máquinas ha facilitado así el conocimiento de las personas.

Los sistemas parcialmente autónomos e inteligentes se han utilizado en tecnología militar desde al menos la Segunda Guerra Mundial, pero los avances en el aprendizaje automático y la IA representan un punto de inflexión en el uso de la automatización en la guerra. Si bien las comunidades militares y de inteligencia de los Estados Unidos están planeando un uso ampliado de la IA en sus carteras, muchas de las aplicaciones más transformadoras de la IA aún no se han implementado (Allen & Chan, 2017). Por ello, en el proceso de integración persona-máquina, en la hibridación que genera *cyborgs* (Scharre & Fish, 2018), es mucho más preocupante la mecanización del pensamiento humano que la humanización del robótico, a pesar de que los medios de comunicación y entretenimiento han hecho hincapié en esta última opción.

Metodología

El presente artículo se basa, inicialmente, en el estudio detallado de los numerosos códigos éticos elaborados por instituciones, empresas y sociedad civil sobre el uso de la IA y que se recoge en diversos documentos y estudios (Gómez-de-Ágreda, 2020). Dichos estudios recogen, además, un análisis minucioso del estado del arte de la tecnología digital aplicada a usos bélicos.

El trabajo plantea, por un lado, analizar, explicar y debatir sobre un fenómeno existente desde hace algunos años, de acuerdo con la literatura científica revisada, como es el auge de la IA en el desarrollo de los conflictos bélicos, abordando las incógnitas sobre sus usos, las estrategias y los modelos cognitivos en su uso, factores que repercutirán en las estrategias de defensa de los países como usuarios de estas tecnologías; por otro, proponer nuevos enfoques, retos e iniciativas que al alimón de la implantación y consolidación de la IA en los conflictos bélicos, deberán tenerse en cuenta para las futuras —y presentes— generaciones de personas. Por ello, la metodología utilizada es descriptiva y exploratoria, explicativa y no experimental, basada en la revisión documental de fuentes sobre IA, situaciones bélicas, ciberguerra, modelos cognitivos, códigos éticos y principios en los conflictos.

Se ha llevado a cabo una exhaustiva revisión bibliográfica centrada en textos, para desarrollar una taxonomía de las aplicaciones bélicas y maliciosas de la IA (Brundage et al., 2018), que prescinde de las características tecnológicas de esta para centrarse en su aplicación operacional. A estos efectos, se han estudiado las doctrinas y estrategias de seguridad y defensa de los principales países con el objeto de identificar las formas de acción empleadas. Los criterios para seleccionar los documentos de referencia se basaron en la temática específica, en las publicaciones indexadas en bases de datos de calidad acreditada y en los cargos de expertos que representan sus autores, considerando que por cuestiones de espacio no pudo incluir a todos. A partir de estos análisis, se buscó extrapolar y abordar las cuestiones éticas (Flores-Vivar & García-Peñalvo, 2023) y filosóficas de la IA que vienen planteando expertos y de organizaciones de todo el mundo, buscando la reflexión, el debate y la prospectiva

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

sobre las profundas implicaciones estratégicas y tácticas que la IA, de modo general, tendrá en el ámbito de la defensa y la ciberseguridad. Los resultados obtenidos no son un conjunto cerrado de opciones, sino que se ramifican, a su vez, en numerosas alternativas susceptibles de ser desarrolladas en otros estudios.

Taxonomía de los usos bélicos de la inteligencia artificial

Un estudio en profundidad de los usos bélicos de la IA (Gómez-de-Ágreda et al., 2019) permite identificar una serie de aplicaciones diferenciadas y elaborar una taxonomía de estas. Resulta casi imposible llevar a cabo un estudio adecuado de la incidencia de la IA en la guerra sin tener en cuenta todas sus distintas manifestaciones, como incorrecto pretender pasar por alto las implicaciones de cada una de ellas en todas las demás y en el conjunto de las herramientas y armamento.

No obstante, los conflictos contemporáneos se libran en muy buena parte fuera de los campos de batalla, incluso en ámbitos no físicos, como el cibernético y el cognitivo. En estos dos entornos se da un uso no menos intenso de la IA con la misma finalidad de alterar la voluntad de los adversarios. En Gómez-de-Ágreda et al. (2021) se estudiaron y categorizaron las herramientas que se emplean para ejecutar operaciones de influencia y desinformación. Su importancia ha quedado de manifiesto en numerosas ocasiones en los últimos años. De ahí la reciente tendencia en las principales fuerzas armadas del mundo a crear mandos específicos para gestionar de forma integrada todas las capacidades cognitivas y fusionarlas con el resto de las herramientas (Deptula, 2022).

La IA encuentra también interesantísimas aplicaciones en la resolución de esos mismos conflictos y en el apoyo a las labores diplomáticas encaminadas a ello. La taxonomía creada en su momento por Parasuraman et al. (2000) se centra más en aspectos técnicos que operacionales y, a pesar de su indudable valor y razonable vigencia, requiere otra clasificación complementaria que recoja los modos de empleo (figura 1).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

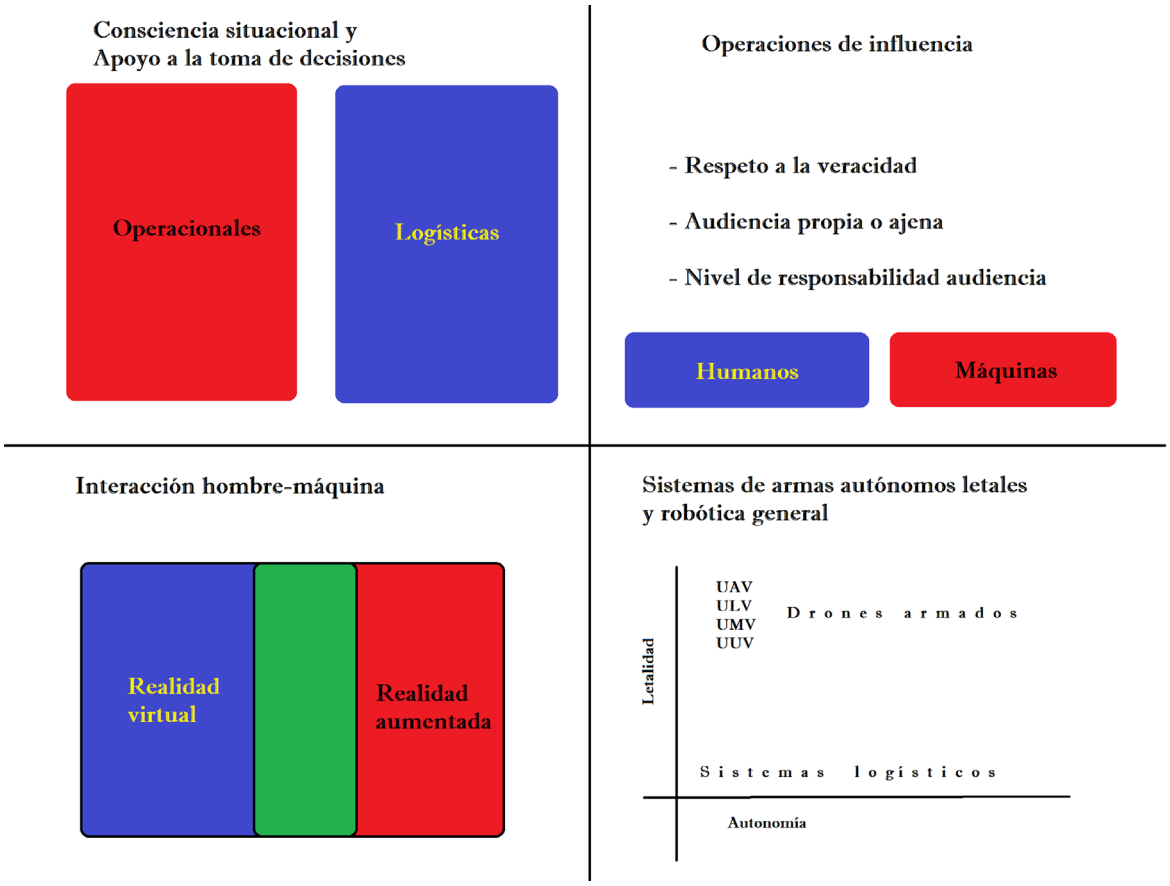

Figura 1. Propuesta de taxonomía de los usos de la inteligencia artificial en operaciones militares

Fuente: elaboración propia.

En realidad, la IA no funciona aislada, sino que se aplica a un conjunto amplio de datos que, en muchos casos, se recopilan a través de miles de sensores —muchas veces guiados también por algoritmos— del llamado *internet de las cosas*. El resultado de la gestión podría dividirse entre aquellos sistemas cuya función es elaborar información extraída de dichos datos y los que se encargan de recomendar —y actuar, en su caso— sobre sistemas lógicos o físicos. En la figura 1 se propone una taxonomía de uso de la IA en operaciones militares, basada en la identificación de las siguientes categorías, en cuanto al modo de empleo de los algoritmos:

- Los dedicados a la provisión de visualizaciones que permiten mejorar la consciencia situacional y la toma de decisiones mediante un análisis aséptico de los datos. Estas decisiones pueden dividirse, a su vez, entre las de carácter operacional[1] y las de tipo logístico, cada una de ellas con una sensibilidad diferente.

1 En este caso, los resultados suelen estar recogidos en lo que se denomina *common operational picture* (COP).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

- Aquellos cuya labor sea la elaboración de contenidos destinados a influir en los destinatarios. Dentro de esta categoría cabría distinguir entre aquellos que lo hacen desde el respeto de los datos originales y los que generan datos o interpretaciones sesgadas para su presentación a la audiencia. Una segunda división diferenciaría entre los destinados a una audiencia propia y aquellos elaborados para ser presentados al adversario, si bien esta subcategoría solo sería aplicable en determinados medios y plataformas. Finalmente, una tercera partición distinguiría entre los diferentes niveles de responsabilidad de la audiencia objetivo (liderazgo único o compartido, nivel ejecutivo…). En esta categoría, y en la primera, se diferencia también entre audiencias humanas o mecánicas, ambas sensibles a la desinformación o al envenenamiento de los datos.
- Aquellas aplicaciones diseñadas para la interacción directa con los sistemas cognitivos humanos y no meramente para la presentación de resultados que deban ser interpretados en función de códigos más o menos complejos, como el lenguaje. Normalmente, irán asociadas con dispositivos capaces de generar señales que transmitan la percepción —o la emoción— sin necesidad de nuevas interpretaciones. Las realidades virtual y aumentada son primeras manifestaciones de estas aplicaciones, que se incrementarán con sistemas neurocientíficos.
- La utilización de los algoritmos para la dirección —o apoyo— de sistemas de armas con mayor o menor autonomía y grado de letalidad. Se incluirían aquí tanto los sistemas logísticos desarmados como aquellos diseñados para ejercer fuerza letal. Los sistemas tripulados de forma remota (tanto sistemas terrestres, navales, submarinos como aéreos y espaciales) solo emplean la IA de forma complementaria en la gestión de los datos y las funciones propias de operación de las plataformas. No obstante, otros sistemas de armas elevan el grado de autonomía en la decisión y la actuación hasta dejar al humano fuera del ciclo de decisión.[2]

Autonomía y letalidad

Mientras que la última de las categorías ha centrado la mayor parte de la atención por parte de la opinión pública, sociedad civil (International Committee of the Red Cross, 2018; Stop Killer Robots, 2018) y de los reguladores (CCW, 2018), cabe argumentar que todas ellas deberían tratarse de un modo similar. Significativamente, no obstante, los códigos éticos generales de la IA —muy especialmente cuando los elaboran instituciones o corporaciones— apenas si mencionan los usos bélicos (Future of Life Institute, 2020; Shahriari & Shahriari, 2017), en lo que cabe interpretar como un intento de reducir la visibilidad este tipo de aplicaciones en beneficio de un rápido desarrollo de la industria.

Desinformación e influencia

La desinformación, si bien no es exclusiva del entorno bélico (Aslama-Horowitz, 2019), alcanza su máximo potencial entre este. Su empleo en la justificación del conflicto, en la cohesión de cada bando y en la afectación de

2 La criticidad dependerá, más que del grado de autonomía del sistema, de aquellas fases de la toma de decisión en las que se aplique. En cualquier caso, incluso grados de autonomía muy limitados pueden escapar a los criterios éticos o legales. En Gómez-de-Ágreda (2020) se profundiza en este debate.

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

la toma de decisiones informada por parte del enemigo, la convirtieron ya en un elemento bélico fundamental mucho antes de la aparición de las modernas técnicas digitales.

Sin embargo, el advenimiento de la red como escenario de convivencia ha abierto nuevos frentes y múltiples posibilidades. Así, aunque sigue sin estar claro el impacto real de las acciones de influencia durante la campaña electoral de Estados Unidos (Allcott & Gentzkow, 2017), la existencia de una duda razonable sobre la posibilidad de un influjo externo condicionó la campaña en 2020.

La manipulación realista de imágenes y videos requiere ahora apenas unas pocas pulsaciones del ratón. La existencia de programas y bases de datos comerciales hacen la labor accesible a casi cualquiera (Gómez-de-Ágreda et al., 2021). La incertidumbre que abre la necesidad de dudar incluso de lo que se está viendo (en forma mediada) puede constituir una coartada plausible para negar evidencias. Es lo que Barnes y Barraclough (2019) y otros denominan el *dividendo del mentiroso*.

En cualquier caso, para sostener la clasificación anterior, se puede recurrir también a los nuevos conceptos doctrinales de la guerra que se están desarrollando en estos momentos. La guerra multidominio y en mosaico (Pulido, 2021) implica el empleo coordinado de todas estas capacidades para conducir físicamente plataformas capaces de recopilar datos de forma autónoma, aplicaciones para extraer inteligencia de esos datos y explotarla en operaciones de influencia,[3] y el uso de plataformas más o menos autónomas para efectuar ataques físicos sobre el adversario.

En el ámbito cognitivo humano

Cabe integrar en esta clasificación del empleo de la IA en la guerra —si bien también tiene un carácter general para todo uso de los algoritmos— las enseñanzas extraídas sobre el funcionamiento del razonamiento humano a partir del estudio de la programación de los algoritmos y su comportamiento y viceversa (Templeton et al., 2022).

Igual que con cualquier otra arma, en el caso de las operaciones de influencia, en el uso de la IA en el campo de batalla es preciso tener en cuenta todos los factores que intervienen. No basta con conocer bien los efectos potenciales de los algoritmos. También es preciso comprender las ventajas e inconvenientes de cada uno de los medios disponibles para la difusión de los contenidos y, por supuesto, estudiar las características de la audiencia que recibirá el mensaje.

El momento actual es de transición generacional. Hay generaciones de veteranos poco inclinados al uso de estas tecnologías —pero, precisamente por ello, altamente vulnerables a sus sutilezas— y jóvenes con mayor conciencia del entorno, pero también con una exposición muy alta.

Preocupantemente, la interacción hombre-máquina ha propiciado un acomodo de la racionalidad humana a los procedimientos —mucho más simplificados— de los algoritmos. Esto es, el humano se ha acomodado a la máquina simplificando su raciocinio. Esto se une a los efectos secundarios del uso de las tecnologías digitales en la generación de audiencias altamente receptivas al relato que procede de fuentes algorítmicas. Diversos filósofos (Han, 2021) y analistas vienen avisando de estos cambios de actitud.

3 En este documento no se está entrando en la distinción entre operaciones de influencia y de desinformación, a pesar de que existen diferencias entre ellas (Torres Soriano, 2022).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

Ya Simon (1971) alertaba sobre el hecho de que un ambiente rico en información genera una merma en la atención. La IA permite el acceso a una cantidad de información tal que se genera lo que Platón denominaba en sus *Diálogos* como una "ilusión de sabiduría", normalmente acrítica. En muchos otros casos, la audiencia busca conscientemente contenidos falseados (Woolley & Joseff, 2020), pero más atractivos visual o lúdicamente. Numerosos estudios demuestran cómo, independiente de la actuación de programas automáticos (*bots*), los contenidos engañosos alcanzan consistentemente una mayor difusión por parte de los usuarios humanos que los verídicos.

Postman (2005) habla de una sociedad entregada a lo lúdico; Debord (2005) la caracteriza como "sociedad del espectáculo", y Marina (2022) alerta contra la búsqueda de la felicidad como bien supremo. El clásico equilibrio entre seguridad y libertad queda subordinado al máximo confort y a la satisfacción instantánea de los deseos. La generación *play again* rechaza el compromiso y la responsabilidad viviendo la realidad como si se tratase de un videojuego de vidas infinitas (Gómez-de-Ágreda, 2019).

La integración de las cuatro categorías se muestra también en la vinculación entre la presentación de resultados agregados sobre grandes bases de datos y las aplicaciones encaminadas a ejercer influencia. La rápida sucesión de generaciones de armas cognitivas aprovecha estas relaciones cruzadas para ir constantemente por delante de la capacidad de reacción de individuos, sociedades y grupos políticos. Así, hace solo unos pocos años se hablaba de un entorno recolector de datos, un capitalismo de vigilancia (Zuboff, 2020). En cambio, la preocupación actual es en relación con una realidad sintética generada en función de las características personalizadas de la audiencia o del efecto uniformador de las tecnologías sobre esta. Lassalle (2022) y otros hablan de un capitalismo digital de sustitución (por contraposición a la mera vigilancia) que proporciona realidades a la medida.

Plataformas y privacidad

En la fase de provisión de datos a los algoritmos se dilucidan dos batallas simultáneas en las que intervienen principalmente actores no estatales, pero que proporcionan las bases para la inteligencia de los Estados. Esta relación simbiótica entre Estados y empresas —y no razones puramente de mercado— es la razón principal de la creación y posterior supervivencia de los grandes monopolios digitales. Como reacción, algunos países han vetado la entrada total o parcial de estas plataformas en sus mercados para favorecer campeones locales que retengan el acceso a los datos. Esto es muy evidente en el caso de las redes sociales y de mensajería instantánea (casos como WeChat, Kakao o Naver), en las que los mismos usuarios suelen proporcionar y vincular entre sí los datos.

La privacidad queda muy diluida en este entorno lúdico, por lo que las empresas que gestionan las redes adquieren gran poder (Veliz, 2020). La gran cantidad de datos proporcionados por millones de usuarios y el alto grado de coherencia entre ellos hace que este sea mucho mayor que el derivado del valor económico de los datos tomados de forma individual. La inmersión que provocan tecnologías como la realidad virtual no hace sino agravar la transparencia del usuario frente a una plataforma en la que el avatar se confunde con su propietario (Mir & Rodríguez, 2020).

En los últimos años han aparecido actores especializados en la interacción con estos avatares de las redes sociales para la generación, difusión y potenciación de desinformación y para llevar a cabo operaciones de influencia a través de ellos. Algunos autores les denominan *advanced persistent manipulators* (APM), en referencia a sus equivalentes cibernéticos (Watts, 2019).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

No es probable, por lo tanto, que estas sociedades paralelas entren en declive salvo, que sea, como queda dicho, para su sustitución por mecanismos más eficientes. La mutación responde a su cambio de rol de "modelos de negocio monetizables (a) modelos de poder hegemonizables" (Lassalle, 2022).

Conclusiones

La aplicación de la IA, incluso cuando tiene ánimo beneficioso, altera la percepción que los humanos tienen de su entorno y de la sociedad. La realidad sintética se superpone o sustituye hoy a buena parte de la interpretación que hacemos de la realidad. La preservación de la dignidad y la libertad humanas exige un esfuerzo adicional que permita disfrutar de las ventajas de la tecnología sin que, por eso, se pierda la esencia de la humanidad. La búsqueda de la optimización y la exigencia continúa de felicidad, comodidad e inmediatez son incompatibles con la naturaleza física a la que seguimos anclados.

La práctica total de las estrategias nacionales de seguridad de los últimos años, con la de Japón como el ejemplo más reciente, destaca cómo se ha diluido la distinción entre las operaciones bélicas y las funciones de seguridad nacional. La continuidad entre política y guerra proclamada por Von Clausewitz (2002) nunca ha sido más real que en la zona gris en la que se desarrolla actualmente la actividad internacional de los Estados.

Se incluyen en esta fusión muchos de los medios empleados en ambas situaciones. La confrontación en los ámbitos cibernético y cognitivo figuran prominentemente entre los que forman parte del continuo de operaciones que abarca la totalidad el espectro, desde las operaciones en tiempo de paz hasta el conflicto bélico abierto y la posterior reconstrucción de la estabilidad.

Para comprender con claridad el nuevo ecosistema en que tienen lugar la cooperación y la competición internacional, es preciso contextualizar de modo correcto la aportación de la tecnología a la transformación, no solo de las tácticas, técnicas y procedimientos militares, sino a la configuración misma de la sociedad sujeto y objeto de aquellas. Ante lo rápidamente evolutivo de los usos de las tecnologías digitales —y de la IA en concreto—, una aproximación ética o normativa a cada uno de ellos sería, amén de inviable, incorrecta.

Los mismos algoritmos que permiten avances sociales y tecnológicos —impensables hace apenas unas décadas— están transformando el modo en que los humanos nos aproximamos a las percepciones y el basamento mismo de nuestras emociones. La dualidad de uso de estas tecnologías implica la necesidad de alejar el foco de los casos concretos para analizar sus efectos en el conjunto de la sociedad. No se trata solo de optimizar el empleo de la IA, sino también de minimizar sus efectos indeseados; aquellos provocados por un diseño imperfecto de nuestros propios programas y aquellos otros generados por la acción adversaria de otras inteligencias o la simple distorsión interesada de los datos en que estas se basan.

Desde el ámbito estrictamente militar, la taxonomía de clasificación de los usos de la IA propuesta debería servir para hacer un mejor uso integrado de los recursos puestos a disposición del desarrollo y adquisición de estas tecnologías, y para el diseño de estrategia, técnicas, tácticas y procedimientos que mejoren su uso propio y la protección frente al de los adversarios. No obstante, todo lo anterior es también susceptible de ser empleado fuera del ámbito militar, con fines maliciosos de carácter criminal. En este caso, su conocimiento debería permitir mitigar los efectos de estas acciones.

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

La conclusión principal que se alcanza es que los países deben tener en cuenta la división de funciones para integrar las capacidades —aprovechando las sinergias existentes— que proporciona cada una con todas las demás. Estudios recientes, que se aproximan también a la utilidad de la IA para apoyar la resolución diplomática de los conflictos gracias a una mejor y más objetiva comprensión de las causas y las posibles soluciones, deberían tomarse como ejemplo de un uso beneficioso de la IA.

Referencias

1. Aguado, J. M. (2020). *Mediaciones ubicuas.* Gedisa.
2. Aguado, J. M., Feijóo, C., & Martínez Martínez, I. J. (2013). *La comunicación móvil hacia un nuevo ecosistema digital.* Gedisa.
3. Allen, G., & Chan, T. (2017*). Artificial Intelligence and National Security: A study on behalf of Dr. Jason Matheny, director of the U.S. Intelligence Advanced Research Projects Activity (IARPA)*. Belfer Center for Science and International Affairs-Harvard Kennedy School.
4. Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, *31*(2), 211-236. https://doi.org/10.1257/jep.31.2.211
5. Aslama-Horowitz, M. (2019). Disinformation as warfare in the digital age: dimensions, dilemmas, and solutions dimensions, dilemmas, and solutions. *Journal of Vincentian Social Action*, *4*(2). https://scholar.stjohns.edu/jovsa/vol4/iss2/5
6. Ayerbe, A. (2020). La ciberseguridad y su relación con la inteligencia artificial. *ARI* (128). https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial.pdf]
7. Baker-Brunnbauer, J. (2023). Introduction. En *Trustworthy artificial intelligence implementation: Business guides on the go*. Springer. https://doi.org/10.1007/978-3-031-18275-4_1
8. Barnes, C., & Barraclough, T. (2019). *Perception Iinception: Preparing for deepfakes and the synthetic media of tomorrow*. The Law Foundation.
9. Bonfanti, M. E. (2020). The weaponisation of synthetic media: What threat does this pose to national security? *ARI*, *93*. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari93-2020-bonfanti-weaponisation-of-synthetic-media-what-threat-does-this-pose-to-national-security
10. Boulanin, V. V. V. (2018). The impact of artificial intelligence on strategic stability and nuclear risk. *Sipri*, *I*(May). https://doi.org/10.2991/icsshe-18.2018.203
11. Boyer, P. (2018). *Minds make societies: How cognition explains the world humans create*. Yale University Press.
12. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., HÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., … Amodei, D. (2018, febrero). *The malicious use of artificial intelligence: forecasting, prevention, and mitigation*. https://arxiv.org/pdf/1802.07228
13. Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., Henke, N., & Trench, M. (2017). *Artificial intelligence: The next digital frontier?* [discussion paper]. McKinsey Global Institute (MGI).

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

14. Calvo-Albero, J. L. (2020). *Implicaciones en el ámbito cognitivo en las operaciones militares*. Centro Superior de Estudios de la Defensa Nacional. https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf
15. CCW. (2018). *Chair's summary of the discussion*. *6*(April), 1-13.
16. Chesney, R., & Citron, D. (2018, 11 de diciembre). Deepfakes and the new disinformation war. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war
17. Debord, G. (2005). *La sociedad del espectáculo*. Pre-Textos.
18. Deptula, D. A. (2022). A new battle command architecture for Joint all-domain operations. *ÆTHER: A Journal of Strategic Airpower & Spacepower*, *1*(1), 51-56. https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/08-Deptula.pdf?source=GovD
19. Flores-Vivar, J., & García-Peñalvo, F. (2023). Reflections on the ethics, potential, and challenges of artificial intelligence in the framework of quality education (SDG4). *Comunicar, 74,* 37-47. https://doi.org/10.3916/C74-2023-03
20. Future of Life Institute. (2020). Asilomar AI principles. *Future of Life Institute*, 1-49. https://futureoflife.org/ai-principles/?submitted=1#confirmation
21. Gartner. (2018, 24 de julio). Hype CYCLe for artificial intelligence, 2018. https://www.gartner.com/en/documents/3883863
22. Gómez-de-Ágreda, Á. (2019). *Mundo Orwell: Manual de supervivencia para un mundo hiperconectado*. Ariel.
23. Gómez-de-Ágreda, Á. (2020). Ethics of autonomous weapons systems and its applicability to any AI systems. *Telecommunications Policy*, *44*(6), 1-15. https://doi.org/10.1016/j.telpol.2020.101953
24. Gómez-de-Ágreda, Á., & Feijoo, C. (2021). Hacia una ética del ecosistema híbrido del espacio físico y el ciberespacio. *Diecisiete* (4), 47-58. https://doi.org/10.36852/2695-4427_2021_04.02
25. Gómez-de-Ágreda, Á., Feijóo, C., & Salazar, I. (2021). Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital: Deep fakes e inteligencia artificial. *El Profesional de la Información*, *30*(2). https://doi.org/10.3145/epi.2021.mar.16
26. Gómez-de-Ágreda, Á., Martínez, J. M., Mohíno Herranz, I., Barragán Montes, R., Marín Gutierrez, F. A., Cubeiro Cabello, E., & Aznar Lahoz, J. L. (2019). *Usos militares de la inteligencia artificial, la automatización y la robótica (IA&R)*. Centro Superior de Estudios de la Defensa Nacional. http://www.ieee.es/contenido/noticias/2019/11/DIEEET04-2019InteligenciaRobotica.html
27. Gómez-López, J. (2019). Tecnologías de la información y los mensajes en los nuevos espectros del conflicto. *Revista de Ciencias de la Comunicación e Información*, (24), 45-56.
28. Han, B. C. (2021). *No-cosas: Quiebras del mundo de hoy*. Taurus.
29. Helmus, T. C. (2022, julio). *Artificial intelligence, deepfakes, and disinformation: A primer.* RAND Corporation. https://doi.org/10.7249/pea1043-1
30. International Committee of the Red Cross. (2018, 3 de abril.). *Ethics and autonomous weapon systems: An ethical basis for human control?* https://www.icrc.org/en/document/ethics-and-autonomous-weapon-systems-ethical-basis-human-control
31. Johnson, J. (2020). Artificial intelligence, drone swarming and escalation risks in future warfare. *RUSI Journal*, *165*(2), 26-36. https://doi.org/10.1080/03071847.2020.1752026

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

32. Lassalle, J. M. (2022, 22 de octubre). Capitalismo digital de sustitución. *La Vanguardia*. https://www.lavanguardia.com/opinion/20221022/8576754/capitalismo-digital-sustitucion.html
33. Leonardo-Oviedo, G. (2004). La definición del concepto de percepción en psicología con base en la teoría Gestalt. *Revista de Estudios Sociales*, *18*, 89-96.
34. Marina, J. A. (2022). *El deseo interminable*. Ariel.
35. Mir, R., & Rodríguez, K. (2020). *If privacy dies in VR, it dies in real life*. https://www.eff.org/deeplinks/2020/08/if-privacy-dies-vr-it-dies-real-life
36. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, *30*(3), 286-297. https://doi.org/10.1109/3468.844354
37. Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes. *Data & Society*, 47. https://site.ieee.org/sagroups-7011/
38. Postman, N. (2005). *Amusing ourselves to death*. Penguin Books.
39. Pulido, G. (2021). *Guerra multidominio y mosaico*. Catarata. https://www.catarata.org/libro/guerra-multidominio-y-mosaico_133474/
40. Scharre, B. P., & Fish, L. (2018, 7 de noviembre). *Human performance enhancement*. Center for a New American Security. https://www.cnas.org/publications/reports/human-performance-enhancement-1
41. Scharre, P. (2019). Killer apps: The real dangers of an AI arms race. *Foreign Affairs*, *98*(3), 135-144. https://www.foreignaffairs.com/articles/2019-04-16/killer-apps
42. Schick, N. (2020, 28 de diciembre). Los "deepfake" no han roto la democracia en 2020; los "cheapfake", sí. *MIT Technology Review*. https://www.technologyreview.es/s/13044/los-deepfake-no-han-roto-la-democracia-en-2020-los-cheapfake-si
43. Shahriari, K., & Shahriari, M. (2017). IEEE standard review. Ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems. *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*, Toronto, ON, Canada, 197-201. https://doi.org/10.1109/IHTC.2017.8058187
44. Simon, H. A. (1971). Designing organizations for an information-rich world. En M. Greenberger (Ed.), *Computers, communications, and the public interest*. John Hopkins University Press.
45. Stop Killer Robots. (2018). *Campaign to stop killer robots*. https://www.stopkillerrobots.org/
46. Templeton, E. M., Chang, L. J., Reynolds, E. A., LeBeaumont, M. D. C., & Wheatley, T. (2022). Fast response times signal social connection in conversation. *Proceedings of the National Academy of Sciences of the United States of America,* 119(4). https://doi.org/10.1073/pnas.2116915119
47. Torres Soriano, M. R. (2022, 28 de junio). *Operaciones de influencia vs. desinformación: Diferencias y puntos de conexión*. Instituto Español de Asuntos Estratégicos, (64). https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operaciones.pdf
48. Tschopp, M. (2019). *Good AI, bad AI - psychological aspects of a dual-use technology.* https://www.academia.edu/40718200/Good_AI_Bad_AI_Psychological_Aspects_of_a_Dual_Use_Technology
49. Veliz, C. (2020). *Privacy is power: Why and how you should take back control of your data*. Transworld.

DISERTACIONES
Comunicación pública y conflictos armados: El papel de la cognición y el algoritmo en los entornos de la Defensa y la Seguridad Nacional
ISSN: 1856-9536
Doi: https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.12804
Volumen 16, Número 2 / Julio-diciembre 2023
Versión PDF para imprimir desde
http://revistas.urosario.edu.co/index.php/disertaciones

50. Von Clausewitz, K. (2002). *De la guerra*. https://www.psicosocial.net/historico/index.php?option=com_docman&view=download&alias=870-de-la-guerra&category_slug=psicologia-y-violencia-politica&Itemid=100225Watts, C. (2019). *Advanced persistent manipulators, part one: The threat to the social media industry - alliance for securing democracy*. https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/
51. Woolley, S., & Joseff, K. (2020). *Demand for deceit: How the way we think drives disinformation*. https://www.ned.org/wp-content/uploads/2020/01/Demand-for-Deceit.pdf
52. Zuboff, S. (2020). *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós.