



ESCUELA SUPERIOR
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

Una nueva guerra. Impacto estratégico de la IA y la ciberguerra.

Luis Alexander Montero Moncada ESDEG - DEEJC

XIII Seminario de la Asociación de Colegios de Defensa Iberoamericanos ACDIA

Versión: Enero/2024 | UNIÓN, PROYECCIÓN, LIDERAZGO

AGENDA

1

Introducción. Nuevos dominios

2

IA y Ciberguerra. Retos para la IE

3

Modelos rusos y chinos

4

Retos para Iberoamérica

5

Comentarios finales

1

Introducción. Nuevos dominios



»» Introducción. Nuevos dominios

Estamos frente a un salto cualitativo nunca antes visto en la historia de la guerra. La actual revolución tecnológica ofrece transformar a fondo la manera en la cual se pelea en el campo de batalla. Hoy no hay trincheras ni tanques solamente.

El esfuerzo principal está en manos de inteligencias artificiales que moldean la percepción de la realidad, deciden cuál es el mejor diseño operacional, escogen las armas más eficientes y hacen cálculos de bajas con la frialdad de un simple algoritmo.

»» Introducción. Nuevos dominios

Estamos de frente a un salto en el cual no sabemos qué resultará cuando aterricemos

“Lo importante no es la caída sino el aterrizaje”



Repensando los dominios de la guerra

Dominio Físico

Tierra

Mar

Aire

Espacio

Dominio Virtual o ciberespacial

Espionaje (Infiltración, recopilación de datos,

Inteligencia Artificial

Sabotaje (Infraestructura crítica militar y civil, contaminación o falsificación de redes, interferencia de señales y uso de software maliciosos)

Destrucción del sistema financiero y de valores

Dominio Cognitivo

Operaciones de información (Medios convencionales y redes sociales)

Operaciones de ideologización

Construcción de la historia y la "verdad"



El Dominio Ciberespacial consiste en todas las comunicaciones interconectadas, la tecnología de la información y otros sistemas electrónicos, redes y sus datos, incluidos los que están separados o son independientes, que procesan, almacenan o transmiten datos.

NATO STANDARD AJP-3.20
ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS

The background features a complex digital interface with a central globe. The globe is overlaid with a network of glowing white lines and nodes, representing global connectivity. Surrounding the globe are various data visualization elements, including bar charts, line graphs, and circular gauges, all rendered in a light blue and white color scheme. The overall aesthetic is clean, modern, and high-tech, suggesting a focus on data analysis and cognitive computing.

Dominio Cognitivo

En el nivel estratégico

La guerra cognitiva es una guerra de ideologías que busca socavar la confianza que subyace en toda sociedad... La desinformación se aprovecha de la vulnerabilidad cognitiva de sus objetivos, aprovechando miedos o creencias preexistentes que los predisponen a aceptar información falsa

NATO DEVELOPED NEW METHODS OF COGNITIVE WARFARE

François du Cluzel. June-November 2020

En el nivel táctico

En el nivel táctico, las operaciones en el dominio cognitivo se dirigen, entre otras cosas, para afectar directamente en el target:

- 1) Comprensión del entorno y realidad situacional
- 2) Memoria, aprendizaje y velocidad cognitiva
- 3) Ciclos de vigilia-sueño, fatiga y estado de alerta
- 4) Control de impulsos y emociones
- 5) Estado de ánimo, ansiedad y autopercepción
- 6) Toma de decisiones
- 7) Confianza y empatía

**NATO DEVELOPED NEW METHODS OF
COGNITIVE WARFARE**

François du Cluzel. June-November 2020

7 Mandamientos de las Fake News

1. Encontrar (e incrementar) las grietas en el adversario
2. Construir una gran mentira. Apostar por la fuerza del rumor (que juegue con la parte emocional del target)
3. No mentir, sino manipular la verdad.
4. Ocultar tu responsabilidad o participación histórica
5. Encontrar replicadores (idiotas útiles)
6. Negación creíble como arquitecto de la operación
7. Construir un timing, con momentos de énfasis y momentos de pausas operacionales

Adam B. Ellick, Adam Westbrook and Jonah M. Kessel • November 12, 2018. The Seven Commandments of Fake News

<https://www.nytimes.com/video/opinion/100000006188102/what-is-pizzagate.html>

11 principios de propaganda. 2GM

- **Principio de simplificación y del enemigo único**

Adoptar una única idea, un único símbolo; Individualizar al adversario en un único enemigo.

- **Principio del método de contagio**

Reunir diversos adversarios en una sola categoría o individuo; Los adversarios han de constituirse en suma individualizada.

- **Principio de la transposición**

Cargar sobre el adversario los propios errores o defectos, respondiendo el ataque con el ataque.

- **Principio de la exageración y desfiguración**

Convertir cualquier anécdota, por pequeña que sea, en amenaza grave.

- **Principio de la vulgarización**

Toda propaganda debe ser popular, adaptando su nivel al menos inteligente de los individuos a los que va dirigida. Cuanto más grande sea la masa a convencer, más pequeño ha de ser el esfuerzo mental a realizar.

- **Principio de orquestación**

La propaganda debe limitarse a un número pequeño de ideas y repetirlas incansablemente, presentadas una y otra vez desde diferentes perspectivas pero siempre convergiendo sobre el mismo concepto. “Si una mentira se repite suficientemente, acaba por convertirse en verdad”.

11 principios de propaganda. 2GM

- **Principio de renovación**

Hay que emitir constantemente informaciones y argumentos nuevos a un ritmo tal que cuando el adversario responda el público esté ya interesado en otra cosa.

- **Principio de la verosimilitud**

Construir argumentos a partir de fuentes diversas.

- **Principio de la silenciación**

Acallar sobre las cuestiones sobre las que no se tienen argumentos y disimular las noticias que favorecen el adversario.

- **Principio de la transfusión**

Operar siempre a partir de un sustrato preexistente, ya sea un mito nacional o un complejo de odios y prejuicios; se trata de difundir argumentos que puedan arraigar en actitudes primitivas.

- **Principio de la unanimidad**

Llegar a convencer a mucha gente que se piensa “como todo el mundo”, creando impresión de unanimidad

Diario Constitucional – Chile.

<https://www.diarioconstitucional.cl/2018/05/30/sobre-los-11-principios-de-la-propaganda-nazi-desarrollados-por-joseph-goebbels-hoy-vigentes-en-las-fake-news/>



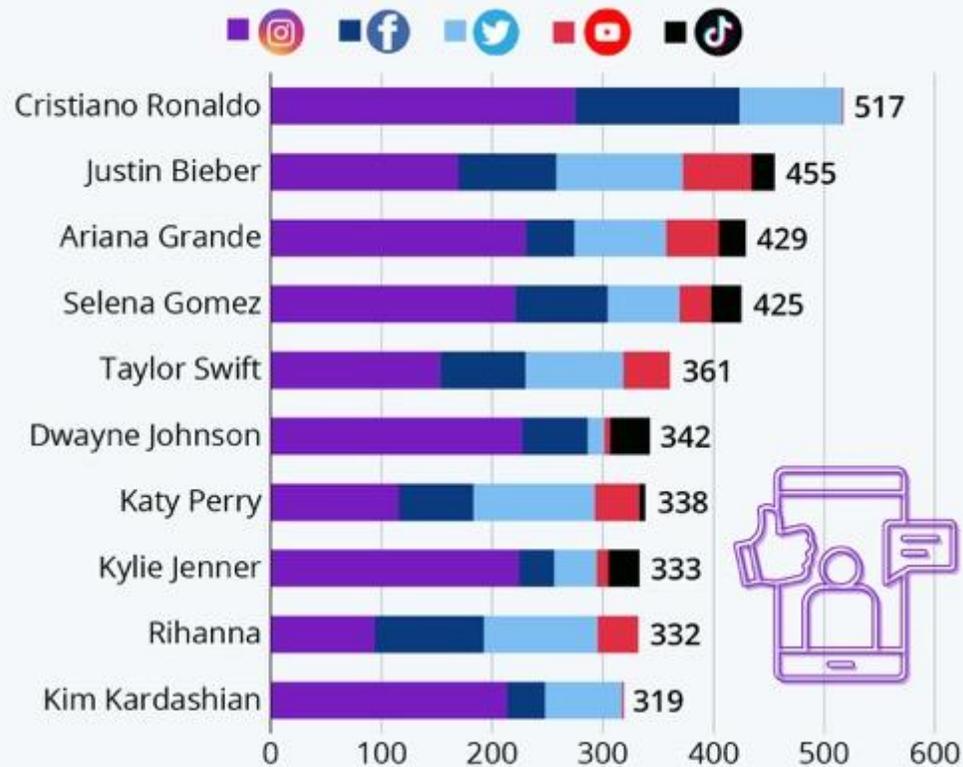
M4C Top tiktokers más seguidos del mundo

2023	2024	Nombre	Seguidores 2024	Variación 2023/2024
1	1	Khabane Lame	161.600.000	4,60%
2	2	Charli D'Amelio	151.700.000	1,34%
3	3	Bella Poarch	93.900.000	1,19%
5	4	MrBeast	92.600.000	24,63%
4	5	Addison Rae	88.700.000	-0,22%
8	6	Kimberly Loaiza	80.600.000	11,63%
6	7	Zach King	80.600.000	10,41%
10	8	TikTok	77.900.000	15,58%
9	9	Burak Özdemir	74.600.000	8,12%
7	10	Will Smith	74.200.000	1,78%

Fuente: elaboración propia a partir de los datos de Digital 2024

Las personas más seguidas en redes

Personas con el mayor número de seguidores en redes sociales (en millones)*



* Redes sociales seleccionadas. Datos de abril de 2021.

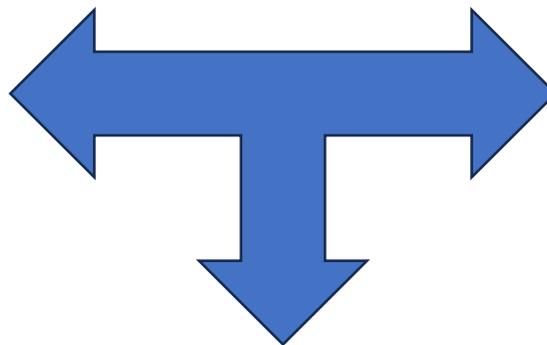
Fuente: Visual Capitalist



statista

Inteligencia
artificial

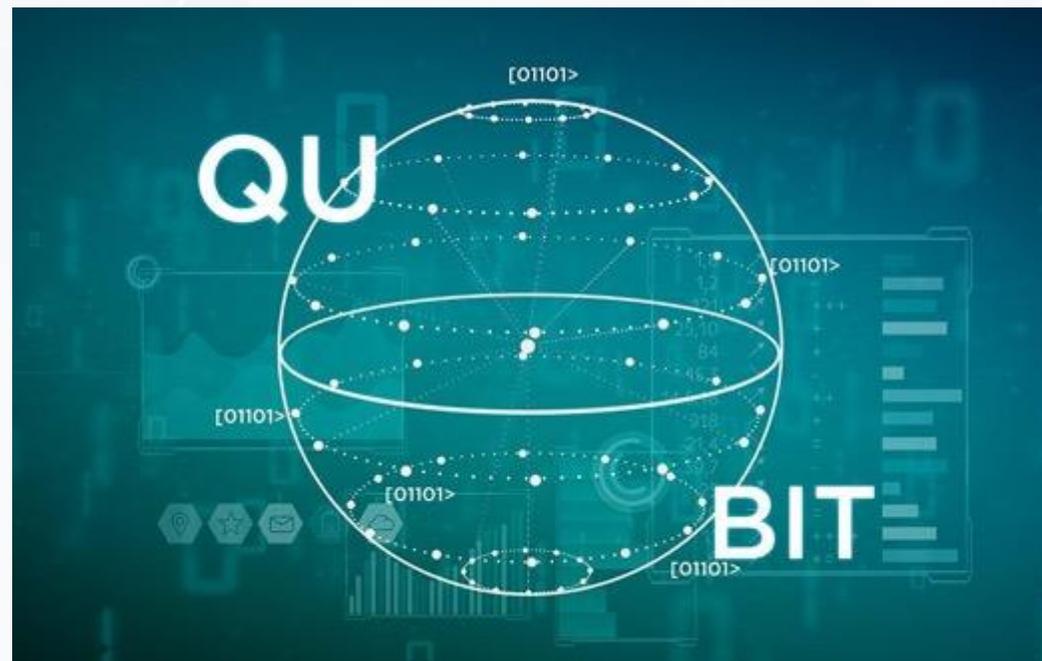
Computación
cuántica



Inteligencia
artificial cuántica

»» IA Cuántica

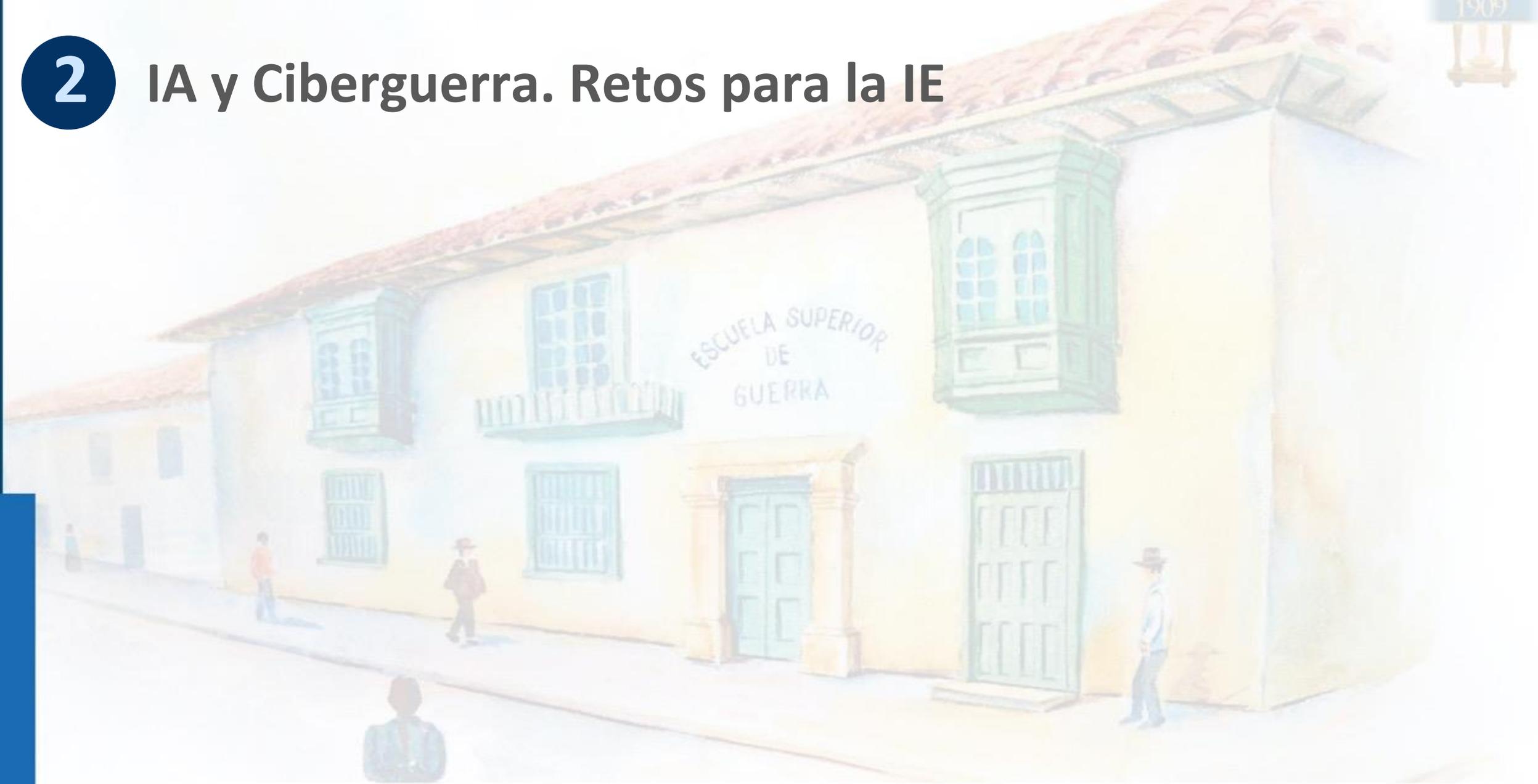
El término “IA cuántica” hace referencia al uso de ordenadores cuánticos para los procesos de los algoritmos de aprendizaje automático. El objetivo es aprovechar la superioridad de procesamiento de la computación cuántica para obtener resultados inalcanzables con tecnologías informáticas clásicas.



Fuente: BBVA Computación Cuántica e IA: una combinación transformacional

2

IA y Ciberguerra. Retos para la IE



»» IA y Ciberguerra. Retos para la IE

Problema

Actualmente hay no solo un desarrollo, sino una clara y preocupante proliferación de nuevas tecnologías, particularmente en los campos de la **inteligencia artificial**, a un ritmo que dificulta que las empresas y los gobiernos establezcan normas relativas a las **libertades civiles, la privacidad y la ética**.

Es probable que la **convergencia** de estas tecnologías emergentes genere avances que podrían conducir al rápido desarrollo de amenazas asimétricas

»» IA y Ciberguerra. Retos para la IE

Problema

Los avances en IA y los nuevos modelos de aprendizaje autónomo están llevando a la IA a su **era industrial**, con lo que se presentan amenazas difíciles de prevenir, como:

- suplantaciones cada vez más sofisticadas
- operaciones de desinformación a gran escala y con un control cada vez mayor del espectro de la narrativa
- el desarrollo de virus informáticos generados por IA
- nuevos sistemas de armas, que pueden incluir no solo ataques cibernéticos más robustos sino todo el espectro de armas NBQ

»» IA y Ciberguerra. Retos para la IE

Problema

Retos del binomio IA-Ciberguerra para la conducción de operaciones militares:

- Ampliación del espectro de lo no atribuible / zona gris
- Automatización del proceso conceptual de identificación de centros de gravedad y de definición de LOEs cada vez más eficientes, pero en el borde de lo legal (Ej. Operaciones de desinformación operaciones políticas o de falsa bandera)
- Automatización del proceso de toma de decisiones militares y desarrollo de algoritmos de gestión de batalla
- Decisión en PSPB
- Conocimiento de la doctrina del adversario y su impacto a la hora de correr juegos de guerra y crear soluciones de batalla
- Riesgo de intrusión en los sistemas propios
- Riesgo de soluciones radicales

MGS 458
TWS 364
STP 197
LTD 657



TRACKING..

N 12' 36' 45"

»» IA y Ciberguerra. Retos para la IE

China

China busca la IA para diseñar ciudades inteligentes, incluyendo sistemas de vigilancia masiva. En este punto, Pekín pone un gran esfuerzo de forma que sus empresas de IA ya son líderes mundiales en reconocimiento de voz e imagen, análisis de vídeo y tecnologías de vigilancia en megaciudades.

Así mismo, la IA china tiene especial concentración en desarrollos relacionados con atención médica, descubrimiento de fármacos (y vacunas) y plataformas de armas inteligentes

»» IA y Ciberguerra. Retos para la IE

China

Buena parte de las IA se están volviendo más sofisticadas, complejizando el ya de por sí difícil mundo de las operaciones en zona gris, donde hay operaciones de influencia digital que intentan afectar las opiniones del público extranjero, influir en las perspectivas de los votantes, cambiar las políticas y crear agitación social y política, entre otras.

Así mismo, los sistemas de IA desarrollados por China se han vuelto mucho más efectivos a la hora de construir falsas acusaciones y todo un prontuario criminal a los disidentes en el extranjero, lo cual deriva en investigaciones policiales locales, visas revocadas, inclusión en listas negras de viajes e incluso, detenciones. Esto abre nuevos conceptos como los de **“Autoritarismo digital”** y **“Represión transnacional”**

»» IA y Ciberguerra. Retos para la IE

Rusia

Por el lado ruso, se está utilizando IA para crear deepfakes cada vez más complejas, de tal manera que cada vez es más difícil detectar el engaño, logrando llevar al error incluso a expertos analistas. Esta capacidad ha sido probada en escenarios de guerra y entornos políticos inestables donde la capacidad que la IA logre un aprendizaje significativo partir de la experiencia es cada vez mayor.

»» IA y Ciberguerra. Retos para la IE

Síntesis

Debido a los retos que ofrece la IA y su binomio con lo ciber, resulta cada vez más difícil lograr una comprensión real del entorno estratégico y operacional. Los analistas de inteligencia deben ser mucho más refinados y robustos, de manera que no conduzcan al error a los tomadores de decisiones.

Así mismo, existe una clara debilidad a la hora de tomar contramedidas y construir mecanismos de protección, en parte porque el entorno global facilita el binomio y porque ante esta amenaza, la brecha tecnológica es mucho más notoria



ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

February 5, 2024



The IC OSINT Strategy 2024-2026

The INT of First Resort:
Unlocking the Value of OSINT

3

Modelos rusos y chinos



Enfoque **ruso** para las operaciones en el dominio cognitivo

Obligar a un líder adversario o a una sociedad a tomar decisiones a favor de Rusia, alterando su percepción del mundo

Objetivos

Características

Doctrina de control reflexivo

La presión cognitiva debe incidir decididamente en la toma de decisiones del objetivo.

La información transmitida debe estar dirigida para influir sobre una decisión específica o una posición

La información debe estar adaptada a la lógica, cultura, psicología y emociones del target

Fundamento

Teoría de la "libertad de decisión" de Niklas Luhmann

NATO DEVELOPED NEW METHODS OF COGNITIVE WARFARE

François du Cluzel. June-November 2020

Enfoque **chino** para las operaciones en el dominio cognitivo

NATO DEVELOPED NEW METHODS OF COGNITIVE WARFARE

François du Cluzel. June-November 2020

Lograr la "superioridad mental" mediante el uso de información para influir en las funciones cognitivas del adversario, desde la opinión pública en tiempos de paz hasta toma de decisiones en tiempos de guerra

Objetivos

Niveles

Doctrina de Mind Superiority

Cognición subliminal: tecnologías que se dirigen a las emociones, la fuerza de voluntad y las creencias de una persona

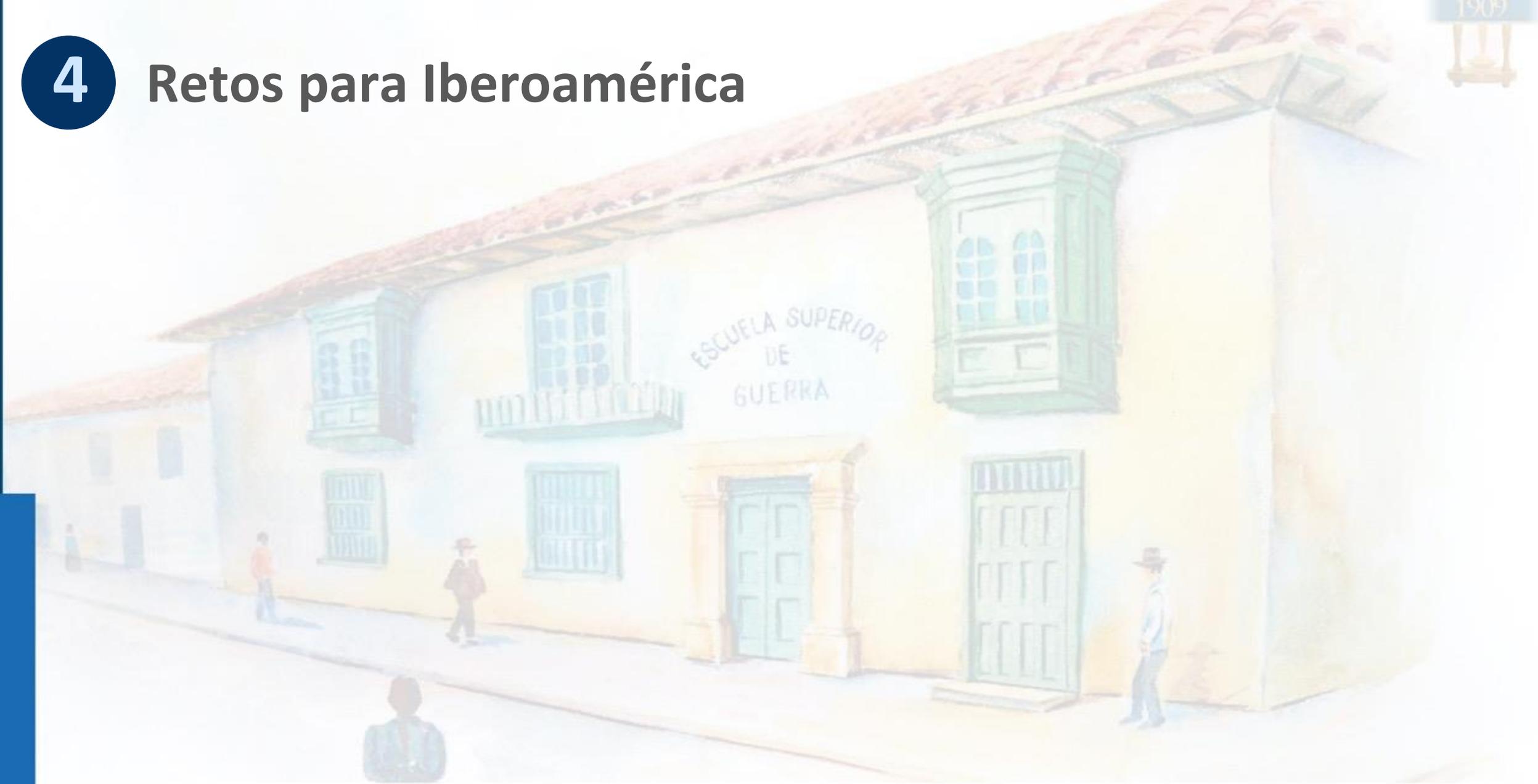
Cognición directa: tecnologías que afectan la capacidad de pensar y funcionar de una persona

Definición

El dominio cognitivo es el campo de batalla para llevar a cabo la penetración ideológica con el objetivo de destruir la moral y la cohesión del enemigo, así como formar o deconstruir sus capacidades

4

Retos para Iberoamérica



Retos para Iberoamérica

- Pobre comprensión de lo estratégico
- Distancia tecnológica con actores relevantes
- Poca comprensión de lo digital y lo ciber incluso dentro de la comunidad de estudios estratégicos
- Estructuras débiles al interior de las FFMM
- Determinismo político y legal
- Visiones aún muy locales
- Sociedades altamente manipulables



Centro
Conjunto de
Desarrollo
de Conceptos

Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)



5

Comentarios finales



Avanzamos decididamente hacia una nueva generación de la guerra. Aquel que se adapte más rápidamente al cambio tendrá más probabilidades de prevalecer



ESCUELA SUPERIOR
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

Preguntas



Escuela Superior
de Guerra



Escuela Superior
de Guerra



@EsdegCol



Escuela Superior
de Guerra



Esdeguecol





ESCUELA SUPERIOR
DE GUERRA

"General Rafael Reyes Prieto"

Colombia



La ***Escuela Superior de Guerra "General Rafael Reyes Prieto"*** está certificada bajo las normas internacionales **ISO 9001:2015** e **ISO 21001:2018**.



Escuela Superior de Guerra
"General Rafael Reyes Prieto"

Colombia

Gracias



Escuela Superior
de Guerra



Escuela Superior
de Guerra



@EsdegCol



Escuela Superior
de Guerra



Esdeguecol

