MASTERCLASS / CICLO «LAS CLAVES ESTRATÉGICAS DE LA DEFENSA DE ESPAÑA EN 2026»

La IA no inventa la desinformación, la multiplica

Nueve claves para entender las nuevas amenazas híbridas

Ponente
Hugo Zunzarren
Especialista en inteligencia y ciberseguridad · Falco Insights

Conversación conducida por
Daniel Villegas
Fundador y director general de LISA Institute

Idea central. La inteligencia artificial no ha inventado la manipulación, pero facilita campañas más veloces, baratas y difíciles de detectar. Las amenazas híbridas combinan dimensiones digitales, económicas, reputacionales y cognitivas. La respuesta exige reconocer patrones, anticipar escenarios, coordinar la seguridad y preservar el análisis crítico de las personas.

01 Las amenazas híbridas combinan vulnerabilidades y vectores

Para Hugo Zunzarren, una amenaza híbrida combina acciones militares, cibernéticas, económicas, reputacionales y cognitivas para alcanzar un objetivo estratégico. Una campaña que perjudica la reputación de una organización puede generar efectos económicos y facilitar ataques posteriores. Esta interdependencia cuestiona la separación tradicional entre seguridad física, ciberseguridad y comunicación. **La protección debe abordarse de forma integral**: identificar riesgos conectados y anticipar cómo pueden explotarse simultáneamente.

02 La IA multiplica la desinformación, pero no la inventa

La manipulación y las operaciones de influencia ya existían antes de la IA generativa. Lo que cambia es su escala: permite producir mensajes, adaptarlos y difundirlos con mayor rapidez y a menor coste. «No cambia la naturaleza de la amenaza, sólo cambia la economía», explicó Zunzarren. En este escenario, la defensa ya no consiste solo en disponer de mejores herramientas. **Aprender, tomar decisiones y reaccionar con agilidad** resulta esencial para no llegar tarde a cada nueva fase de la operación.

03 La guerra cognitiva busca condicionar nuestras decisiones

Las operaciones cognitivas no persiguen necesariamente destruir infraestructuras ni robar datos: pueden intentar modificar percepciones, actitudes y comportamientos sin que las personas identifiquen la manipulación. Una narrativa sostenida puede terminar influyendo en ideas que el receptor considera propias. Zunzarren situó la **resiliencia cognitiva** en el centro de la respuesta: reconocer sesgos, contrastar información y conservar la capacidad de decidir con autonomía, aunque no sea posible impedir todos los intentos de influencia.

04 Hay que estudiar la operación, no cada mensaje por separado

Analizar publicaciones o vídeos aislados puede ocultar el funcionamiento real de una campaña. Zunzarren habló de **«orquestas sin director»**: múltiples actores pueden reforzar una misma narrativa por sus propios intereses, sin instrucciones explícitas. El reto analítico es reconocer las conexiones entre emisores, comunidades y contenidos. Más que centrarse en quién comparte un mensaje concreto, conviene identificar **cómo se propaga una narrativa, qué patrón común muestra y qué comportamiento pretende inducir**.

05 Atribuir una campaña es especialmente complejo

Identificar al responsable de una operación de influencia exige prudencia. Un actor puede alterar sus procedimientos al saberse observado o imitar a otro para desviar la atribución. Zunzarren cuestionó los diagnósticos que adjudican automáticamente una campaña a un país por el parecido de sus técnicas. Propuso trabajar con hipótesis, evidencias, objetivos estratégicos y patrones de comportamiento. **Anticipar la siguiente fase de la amenaza puede ser más útil para protegerse que atribuirla de inmediato**.

06 Los cambios de difusión pueden revelar una manipulación

Los aumentos repentinos de alcance, los cambios de ritmo de publicación o de estilo y la convergencia acelerada de mensajes hacia una misma conclusión pueden ser señales de alerta. Una conversación inicialmente espontánea también puede ser amplificada deliberadamente. Por eso, no basta con buscar cuentas automatizadas: hay que seguir el movimiento de las narrativas entre comunidades y usuarios reales. El análisis debe incluir asimismo los rumores que circulan fuera de Internet y luego se trasladan al entorno digital.

07 Ciberseguridad y protección reputacional deben coordinarse

Las amenazas híbridas desdibujan la separación entre equipos de ciberseguridad, inteligencia, comunicación y gestión de crisis. Una operación informativa puede causar pérdidas económicas, explotar debilidades organizativas o alterar decisiones internas. Zunzarren defendió elaborar hipótesis y escenarios, identificar indicadores tempranos y vincular las capacidades de los centros de operaciones de seguridad con las del análisis reputacional y cognitivo. **La prioridad es reducir los puntos ciegos y responder con rapidez y coordinación**.

08 La IA puede ayudar al analista, no sustituir su criterio

La inteligencia artificial acelera tareas y facilita el tratamiento de información, pero sus conclusiones pueden contener errores convincentes, sesgos o datos contaminados. El especialista insistió en comprobar las fuentes, evaluar la calidad de los datos y cuestionar las hipótesis propias, incluso tratando de refutarlas antes de aceptarlas. **La automatización mejora la eficiencia, pero la verificación y la responsabilidad del análisis deben seguir siendo humanas**.

09 CORTEX y el pensamiento crítico ante las nuevas amenazas

La sesión presentó **CORTEX**, un marco para organizar técnicas de manipulación, sesgos cognitivos y fases de las operaciones de influencia. Su finalidad es facilitar el reconocimiento de patrones y la anticipación de movimientos. Daniel Villegas explicó que se trabajaba en una asociación sin ánimo de lucro para compartir el marco, con participación de LISA Institute y Falco Insights. Zunzarren cerró alertando del riesgo de aceptar las respuestas de la IA como opiniones propias. **La formación interdisciplinar y la autonomía intelectual seguirán siendo fundamentales**.

La conclusión para empresas e instituciones

La defensa frente a la desinformación no depende solo de nuevas tecnologías. Requiere **inteligencia, coordinación, anticipación y pensamiento crítico**. La ventaja estratégica está en analizar, contrastar y utilizar la información sin renunciar a la autonomía de decisión.

> **«No cambia la naturaleza de la amenaza, sólo cambia la economía».**
>
> Hugo Zunzarren · Masterclass del 28 de septiembre de 2026

Documento de síntesis elaborado a partir del artículo de LISA News sobre la Masterclass del 28 de septiembre de 2026, organizada por LISA Institute con el apoyo de la Secretaría General de Política de Defensa (SEGENPOL) y DICOES. Las valoraciones se atribuyen a los participantes. Esta síntesis editorial no sustituye la grabación de la sesión.

Más información: www.lisanews.org