.

Nota Editorial

> HAL 9000: "I'm sorry Dave, I'm afraid I can't do that. (...) I know that you and Frank were planning to disconnect me and I'm afraid that's something I cannot allow to happen". [1]

En las últimas dos décadas la inteligencia artificial (IA) ha venido transformando el ámbito de defensa y seguridad con impactos tanto a nivel estratégico como operativo. Se han implementado sistemas de ciberseguridad automatizados con herramientas avanzadas para el análisis y procesamiento de datos. Esto ha permitido identificar patrones ocultos y predecir escenarios futuros con mayor precisión, al mismo tiempo que se redefinen políticas de prevención y respuesta ante amenazas complejas y diversas. En este contexto dinámico es que los artículos presentados en el décimo volumen de Hemisferio adquieren especial relevancia.

Los trabajos aquí publicados analizan algunos de los problemas y estrategias necesarias para lograr una mejor defensa y resiliencia. Las naciones que tendrán ventajas competitivas en un plazo de 10 años serán aquellas que hoy están logrando adaptarse con relativa rapidez a los nuevos y disruptivos usos de la IA, ya sea en la defensa y seguridad como en la economía en general. Tal como en el film de Stanley Kubrick, las nuevas tecnologías serán un elemento clave en la toma de decisiones, no obstante, los desafíos éticos y de seguridad inherentes.

La creciente sofisticación de la IA y su uso en ataques cibernéticos dibuja un escenario único en la actualidad. El artículo de Eduardo Cunha nos brinda un análisis de la ciberguerra y el terrorismo cibernético, a través de la invasión rusa en Ucrania como caso de estudio. Comprender bien estos fenómenos permitiría diseñar estrategias de mitigación más efectivas para preservar las infraestructuras críticas y la población civil.

Claudio Duarte Faria también se adentra en el mismo campo analítico, pero haciendo énfasis en el rol de la educación en ciberseguridad y la creación de políticas públicas centradas en las personas. El objetivo es proteger a la población contra

[1] Un fragmento del film de 1968: "2001: A Space Odyssey" dirigido por Stanley Kubrick. https://www.youtube.com/watch?v=ARJ8cAGm6JE

eventuales influencias psicológicas y evitar que ésta sea usada como arma al servicio de atacantes en el ciberespacio. En este sentido propone una revisión de las estrategias nacionales de ciberseguridad en la región para que se incluya a la población como "infraestructura crítica". Una mejor protección y resiliencia ante las ciberamenazas requiere un marco político y normativo acorde con los nuevos tiempos.

La evolución tecnológica, donde se incluye la IA, las redes sociales y la hiperconectividad han dado cuerpo al concepto de guerra cognitiva, tal como nos plantea Mario Brasil do Nascimento. El autor plantea el desafío de cómo proteger las democracias sin tender hacia el autoritarismo y restringir la libertad de expresión. Este tercer artículo resalta que al comprender mejor esta amenaza y sus condicionantes es posible que se transforme la defensa cognitiva en una oportunidad que derive en una cooperación interamericana más fortalecida.

En el ámbito de la toma de decisiones la IA juega un rol fundamental. Fabio Nogueira de Miranda analiza cómo los estudios de futuro permiten un proceso de optimización en las políticas públicas frente a un escenario incierto y voluble. Su abordaje sobre las seis fases del ciclo proporciona un marco lo suficientemente flexible como para implementar los estudios de futuro a la planificación y ejecución de las políticas de gobierno. Este enfoque prospectivo aporta a la gestión de amenazas y oportunidades en defensa y seguridad, principalmente a partir de la irrupción de la IA.

Finalmente, Francelmo Araujo Costa estudia las fallas y efectos del concepto de anualidad presupuestaria en los proyectos de inversión en defensa, que por su naturaleza son de largo plazo. Con Brasil como ejemplo, el autor hace recomendaciones para minimizar la falta de previsibilidad y mejorar el uso de los recursos públicos. Este análisis contribuye a garantizar la continuidad y eficiencia de los proyectos estratégicos en defensa de forma tal que logren cumplir con los objetivos de la Política Nacional de Defensa. Este es otro de los campos en los que la IA está siendo empleada, y pudiera complementar los esfuerzos normativos por el uso más eficiente de los recursos.

En conjunto, estos trabajos ofrecen una visión comprehensiva de los desafíos y oportunidades en la interconexión de la ciberseguridad, la guerra cognitiva, y la gestión de políticas públicas y proyectos de inversión de defensa. Con ellos queda la invitación hecha a la reflexión sobre la relevancia de contar con una estrategia integrada y colaborativa ante las actuales amenazas.

.

Para los países de la región, garantizar la resiliencia y seguridad nacional es un imperativo, especialmente en un contexto marcado por la vertiginosa evolución tecnológica y la irrupción de la inteligencia artificial.

Mirlis Reyes Salarichs, Ph.D.
Editora Ejecutiva