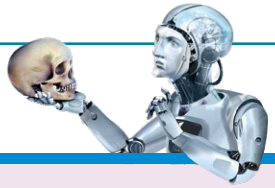
CAVILACIONES SEGURAS



Defensa y ciber: la innovación sucede en la zona liminal

En el contexto geopolítico actual, Europa se enfrenta a un escenario que exige una respuesta coordinada, innovadora y eficaz para enfrentar los crecientes riesgos y amenazas a su seguridad. Nos habíamos dormido un poco pensando que "nuestro primo el de Zumosol" ya nos protegía. Fruto de esta realidad, el viejo continente está embarcándose en el plan ReArm, un macroproyecto de rearme continental, en el que la ciberdefensa y la ciberseguridad emergen como pilares fundamentales de la nueva estrategia de defensa común europea. El plan ReArm incluye un dominio denominado "inteligencia artificial, cuántica, ciber y guerra electrónica". El objetivo es implementar una verdadera unión de defensa europea. Una inversión de 800.000 millones de euros. Confirma claramente la prioridad que Europa concede a este desafío.

El presupuesto del Ministerio de Defensa de España, prorrogado automáticamente desde 2023, asciende inicialmente a 14.000 millones.

Si bien Internet tiene un origen militar, gracias al "inagotable" presupuesto del Departamento de Defensa de EE.UU., hace ya cinco décadas, hoy el reto reside en la militarización de tecnologías civiles ya maduras para reforzar la seguridad de infraestructuras críticas, el sector logístico y otros ámbitos prioritarios

Parece que el objetivo, uniendo otras partidas e inyecciones adicionales, es alcanzar los 30.000 millones de euros para 2025. De ellos, un 10% se dedicará a tecnologías de telecomunicación y seguridad, alcanzando los 3.000 millones. La protección de infraestructuras críticas y servicios esenciales se incluye en este plan.

Si bien Internet tiene un origen militar, gracias al "inagotable" presupuesto del Departamento de Defensa de los Estados Unidos, hace ya cinco décadas, hoy el reto reside en la militarización de tecnologías civiles ya maduras para reforzar la seguridad de infraestructuras críticas, el sector logístico y otros ámbitos prioritarios. Esta convergencia demuestra que la frontera entre defensa militar y el mundo civil es cada vez más difusa y que la innovación tiene lugar en este terreno liminal. ReArm también incluye conceptos de soberanía digital e independencia energética.

Los profesionales involucrados en defensa y ciberseguridad tendrán una responsabilidad histórica: diseñar esta nueva plataforma europea de defensa: un sistema de sistemas, integrado por proyectos que engloban múltiples campos en los que la ciberseguridad aparece, no sólo como requisito imprescindible para proteger los nuevos sistemas de armamento, sino además como una dimensión a proteger y desde la que se puede también atacar. Una colaboración estrecha entre expertos civiles y militares puede proporcionar valor en ambos mundos.

Un perfil profesional versátil y multidisciplinar

Aquí emerge la necesidad de que los expertos en ciberseguridad posean un perfil profesional versátil y multidisciplinar. Curioso: esta recomendación ya aparece en mi primer libro publicado en 2010. Una formación integral que cree "personas del Renacimiento": profesionales capaces de comprender no solo la tecnología, sino también los aspectos estratégicos, legales y sociales en juego, lo que será clave para responder a las amenazas actuales y futuras.

Se abren caminos para el desarrollo de talento y conocimiento directamente vinculados con los actuales desafíos de Europa. Mi consejo a los actuales estudiantes de ciberseguridad: solucionen con sus trabajos de fin de grado o, incluso, con su doctorado industrial, los problemas tecnológicos, sociales y de ciberseguridad que las empresas europeas de defensa enfrentan actualmente al implementar este plan ReArm.

El éxito de este empeño dependerá, sin duda, del capital humano único y excepcional con que aún contamos en Europa, cuya formación, motivación y compromiso es el motor decisivo del futuro.

Dr. Alberto Partida
linkedin.com/in/albertopartida