

Resumen

El crecimiento acelerado de la tecnología, la proliferación de la informática en todas las instituciones del Estado, empresas, banca, industrias, ámbito militar, grupos sociales, población en general; han dado origen al surgimiento de un nuevo dominio (escenario) a nivel mundial denominado el ciberespacio; y con este han surgido múltiples amenazas que han conllevado a la violación de medidas de seguridad informática con el fin de obtener información de inteligencia gubernamental, militar, industrial, económica, científica, ataques a infraestructuras críticas, páginas web, uso de redes sociales como WhatsApp, Telegram para influir en la población y causar caos interno.

Conscientes de la complejidad de este dominio especial y transversal al resto de dominios conocidos, el alto volumen de ciberamenazas y factores de riesgo que deben ser enfrentados, eliminados o reducidos, tanto en el ámbito interno como externo en el ciberespacio y que atentan contra la Soberanía e Integridad Territorial y Seguridad Interna, hacen necesario que el Ejército integre dentro de su organización las políticas y estrategias para la defensa y protección de este nuevo dominio, en concordancia con las adoptadas por el Ministerio de Defensa y el Comando Conjunto de las Fuerzas Armadas.

Palabras clave:

- **CIBERESPACIO**
- **CIBERDEFENSA**
- **OPERACIONES DE DEFENSA, EXPLORACIÓN Y RESPUESTA**

Abstract

The accelerated growth of technology, the proliferation of information technology in all State institutions, companies, banks, industries, the military, social groups, the general population; They have given rise to the emergence of a new domain (scenario) at the world level called cyberspace; And with this, multiple threats have emerged that have led to the violation of computer security measures in order to obtain government, military, industrial, economic, scientific intelligence information, attacks on critical infrastructures, web pages, use of social networks such as WhatsApp , Telegram to influence the population and cause internal chaos.

Aware of the complexity of this special domain and transversal to the rest of known domains, the high volume of cyber threats and risk factors that must be faced, eliminated or reduced, both internally and externally in cyberspace and that threaten Sovereignty and Territorial Integrity and Internal Security, make it necessary for the Army to integrate within its organization the policies and strategies for the defense and protection of this new domain, in accordance with those adopted by the Ministry of Defense and the Joint Command of the Armed Forces.

Keywords:

- **CYBERSPACE**
- **CYBER DEFENSE**
- **DEFENSE OPERATIONS, EXPLORATION AND RESPONSE**