Resumen

La ciberdefensa militar permite a las fuerzas armadas de un país, ejecutar ciberoperaciones en el quinto dominio del campo de batalla, la Fuerza Terrestre del Ecuador en su ámbito de acción, requiere ejecutar la defensa y exploración de sus sistemas de información, bases de datos y redes de comunicación de datos y en cualquier momento y con orden la respuesta a un ataque ciberespacial de una amenaza híbrida, interestatal o internacional. El nuevo escenario estratégico exige el desarrollo de la capacidad ciberespacial en cada una de las ramas de las Fuerzas Armadas como componentes de las operaciones militares conjuntas, es por eso que este trabajo de investigación permitirá al ejército ecuatoriano, disponer de un análisis prospectivo de la ciberdefensa con proyección al año 2033, proporcionando una orientación para el incremento del nivel de madurez de esta capacidad de una manera integral y organizada, mediante la ejecución de las estrategias planteadas para alcanzar un posible escenario apuesta. Para analizar este fenómeno de estudio, se aplicará la herramienta prospectiva de Godet que se desarrolla en tres fases: inicialmente se construirá una línea base que se puede obtener del análisis del macroambiente y microambiente, posteriormente se definen las variables estratégicas con la herramienta ábaco de Regnier y se construyen los escenarios prospectivos en la matriz morfológica, finalmente se desarrollan las estrategias de la ciberdefensa en la Fuerza Terrestre, para obtener los resultados que permitan generar respuestas a los problemas detectados en el estudio del futuro.

Palabras clave: ciberoperaciones, ciberdefensa, estudio prospectivo, estrategias.

Abstract

Military cyber defense allows the armed forces of a country to execute cyber operations in the fifth domain of the battlefield, the Ecuadorian Land Force in its field of action, requires executing the defense and exploration of its information systems, databases, and data communication networks and at any time and with order the response to a cyberspace attack of a hybrid, interstate, or international threat. The new strategic scenario requires the development of cyberspace capacity in each of the branches of the Armed Forces as components of joint military operations, which is why this research work will allow the Ecuadorian army to have a prospective analysis of cyber defense. with a projection to the year 2033, providing guidance for increasing the level of maturity of this capacity in a comprehensive and organized way, through the execution of the strategies proposed to achieve a possible bet scenario. To analyze this study phenomenon, Godet's prospective tool will be applied, which is developed in three phases: initially, a baseline will be built that can be obtained from the analysis of the macroenvironment and microenvironment, then the strategic variables are defined with the Régnier abacus tool. and the prospective scenarios are built in the morphological matrix, finally the cyber defense strategies are developed in the Land Force, to obtain the results that allow generating answers to the problems detected in the study of the future.

Keywords: cyber operations, cyber defense, prospective study, strategies.