Resumen

El presente trabajo titulado “Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del comando de ciberdefensa hasta el 2022”, realizó un trabajo investigativo aplicando una metodología exploratoria, descriptiva y correlacional con enfoque cuantitativo y planteó la hipótesis que afirma que a partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje. Se propuso como objetivo ejecutar un análisis de la capacidad de FF. AA para utilizar las operaciones militares del ciberespacio y los medios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022. A través de las encuestas a 125 oficiales, se pudo concretar la falta de equipo del que carece FF. AA para el control del ciberespacio, así como la capacitación adecuada. Existe además un desconocimiento del 82% de las Amenazas Persistentes Avanzadas cuya intervención están relacionadas directamente con el ciberespacio. Para determinar las estrategias, se trabajó con el análisis FODA, concluyendo con las Matrices EFE y EFI. Al validar las matrices se definió que las estrategias ofensivas son las específicas para este propósito. De manera concluyente se recomienda establecer programas y proyectos de I+D+i propios de FF. AA para implementar sistemas de información y comunicación seguros, mejorar la interoperabilidad interna y externa bajo normas y estándares internacionales.

Palabras clave: ciberespacio, cibersabotaje, ciberespionaje, ciberseguridad, ciberdefensa

Abstract

The present work entitled "Analysis of the operations of the Ecuadorian Armed Forces in cyberspace and the necessary means to counteract cyber espionage and cyber sabotage since the creation of the cyber defense command until 2022", carried out an investigative work applying an exploratory, descriptive and correlational with a quantitative approach and raised the hypothesis that states that from the creation of the Cyber Defense Command until 2022, the analysis of the capacity of the Armed Forces. to use the military operations of cyberspace will allow to face cyber espionage and cyber sabotage. It was proposed as an objective to carry out an analysis of the capacity of FF. AA to use military cyberspace operations and the means to counter cyber espionage and cyber sabotage from the creation of the Cyber Defense Command until 2022. Through surveys of 125 officers, it was possible to specify the lack of equipment that the FF lacks. AA for the control of cyberspace, as well as adequate training. There is also an ignorance of 82% of Advanced Persistent Threats whose intervention is directly related to cyberspace. To determine the strategies, we worked with the SWOT analysis, concluding with the EFE and EFI Matrices. When validating the matrices, it was defined that the offensive strategies are the specific ones for this purpose. Conclusively, it is recommended to establish FF own R&D&I programs and projects. AA to implement secure information and communication systems, improve internal and external interoperability under international norms and standards.

Keywords: cyberspace, cyber sabotage, cyberespionage, cybersecurity, cyber defense